UNIVERSIDADE FEDERAL DO MARANHÃO

Programa de Pós-Graduação em Ciência da Computação

André Luiz Almeida Cardoso

Um Modelo de Gestão de Identidades para Cidades Inteligentes Baseado na Tecnologia Blockchain

São Luís
2024

André Luiz Almeida Cardoso

Um Modelo de Gestão de Identidades para Cidades Inteligentes Baseado na Tecnologia Blockchain

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação - da Universidade Federal do Maranhão, como requisito para obtenção do título de Mestre em Ciência da Computação.

Universidade Federal do Maranhão – UFMA

Programa de Pós-Graduação em Ciência da Computação

UFMA Orientador: Prof. Dr. Francisco José da Silva

Unifesp Co-orientador: Prof. Dr. Arlindo Flavio da Conceição

São Luís

2024

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Almeida Cardoso, André Luiz.
Um Modelo de Gestão de Identidades para Cidades Inteligentes Baseado na Tecnologia Blockchain / André Luiz Almeida Cardoso. - 2024.
77 f.

Coorientador(a) 1: Arlindo Flavio da Conceição.
Orientador(a): Francisco José da Silva e Silva.
Dissertação (Mestrado) - Programa de Pós-graduação em Ciência da Computação/ccet, Universidade Federal do Maranhão, São Luis - Ma, 2024.

1. Gestão de Identidade. 2. Cidades Inteligentes. 3. Blockchain. 4. Hyperledger Fabric. 5. Iot. I. da Conceição, Arlindo Flavio. II. da Silva e Silva, Francisco José. III. Título.

André Luiz Almeida Cardoso

Um Modelo de Gestão de Identidades para Cidades Inteligentes Baseado na Tecnologia Blockchain

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação - da Universidade Federal do Maranhão, como requisito para obtenção do título de Mestre em Ciência da Computação.

Trabalho aprovado. São Luís, 30 de Agosto de 2024:

Orientador: Prof. Dr. Francisco José da Silva
Orientador
Universidade Federal do Maranhão

Prof. Dr. Arlindo Flavio da Conceição
Coorientador
Universidade Federal de São Paulo

Prof. Dr. Luciano Reis Coutinho
Examinador Interno
Universidade Federal do Maranhão

Prof. Dr. Daniel Macêdo Batista
Examinador Externo
Universidade de São Paulo

São Luís
2024

Agradecimentos

Agradeço primeiramente a Deus, pela saúde e oportunidade de chegar até aqui. A minha família, que sempre me apoiou incondicionalmente. Aos mestres que me guiaram e me inspiraram ao longo dessa caminhada. E aos colegas de trabalho que tive o prazer de conhecer o longo destes anos.

Resumo

Cidade Inteligente é um paradigma capaz de atenuar os problemas causados pela urbanização, transformando o ambiente da cidade em algo mais sustentável. Para isso, utiliza-se tecnologias da informação e comunicação para conectar os diferentes atores no contexto de uma cidade. A Internet das Coisas (IoT) é vista como uma das tecnologias-chave para implementação deste paradigma, através dela é possível perceber e atuar sobre o espaço da cidade. Assim como em qualquer sistema computacional a segurança da informação é fundamental, sem mecanismos de segurança torna-se impossível desenvolver e implantar aplicações de cidades inteligentes. A gestão de identidades se apresenta como uma solução para criar um ecossistema seguro para o desenvolvimento de aplicações de cidades inteligentes. A identificação dos diversos atores envolvidos na cidade tais como entidades administrativas do poder municipal, dispositivos de IoT, provedores de serviços e usuários oferece meios para o desenvolvimento de mecanismos de segurança para os serviços da cidade. Esta dissertação apresenta um modelo para gestão descentralizada de identidades baseado em *blockchain*, especificamente voltado para o contexto das cidades inteligentes. Adicionalmente, explorou-se o modelo para desenvolver uma infraestrutura de segurança integrada a uma plataforma de *middleware* para cidades inteligentes. A plataforma *Hyperledger Fabric* foi utilizada como *blockchain* para implementação do modelo. Os experimentos realizados avaliam o custo computacional em termos de consumo de memória e processamento ao adotar-se o modelo proposto, os resultados demonstram a aplicabilidade do modelo e mensuram o custo de adoção.

Palavras-chave: Gestão de Identidade, Blockchain, *Hyperledger Fabric*, IoT, Cidades Inteligentes.

Abstract

Smart City is a paradigm capable of mitigating the problems caused by urbanization, transforming the city's environment into something more sustainable. To achieve this, information and communication technologies are used to connect the different actors in the city's context. The IoT is seen as one of the key technologies for implementing this paradigm, enabling the perception and action over the city space. As in any computer system, information security is fundamental; without security mechanisms, it becomes impossible to develop and deploy smart city applications. Identity management presents itself as a solution to create a secure ecosystem for the development of smart city applications. Identifying the various actors involved in the city, such as municipal administrative entities, IoT devices, service providers, and users, offers means for developing security mechanisms for city services. This dissertation presents a model for decentralized identity management based on *blockchain*, specifically aimed at the context of smart cities. Additionally, the model was explored to develop a security infrastructure integrated with a *middleware* platform for smart cities. The *Hyperledger Fabric* platform was used as the *blockchain* for implementing the model. The experiments conducted evaluate the computational cost in terms of memory consumption and processing when adopting the proposed model, with the results demonstrating the model's applicability and measuring the cost of adoption.

Keywords: Identity Management, *Blockchain*, *Hyperledger Fabric*, IoT, *Smart City*.

Lista de ilustrações

Lista de tabelas

Lista de Siglas

ACM *Association for Computing Machinery.*

BFT *Byzantine Fault Tolerance.*

CI Cidade Inteligente.

CIs Cidades Inteligentes.

DAG *Directed Acyclic Graph.*

DLT *Distributed Ledger Technology.*

DPoS *Delegated Proof of Stake.*

ECC *Elliptic-curve cryptography.*

Gb *Gigabyte.*

GPS *Global Positioning System.*

IAM *Identity and Access Management.*

IdM *Identity Management.*

IdMS *Identity Management System.*

IEEE *Institute of Electrical and Electronics Engineers.*

IoT Internet das Coisas.

IP Internet Protocol.

IPFS *The InterPlanetary File System.*

JWK *JSON Web Key.*

JWT *JSON Web Token.*

MAC Media Access Control.

Mb *Megabyte.*

p2p *Peer-to-Peer.*

PBFT *Practical Byzantine Fault Tolerance.*

PoA *Proof of Authority.*

PoB *Proof of Burn.*

PoC *Proof of Capacity.*

PoS *Proof of Stake.*

PoW *Proof of Work.*

RAM *Random Access Memory.*

RSA Rivest-Shamir-Adleman.

SBSEG Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais.

SSI *Self-Sovereign Identity.*

TIC Tecnologias de Informação e Comunicação.

TLS *Transport Layer Security.*

UUID *Universal Unique Identifier.*

WSN *Wireless Sensor Network.*

Sumário

1 Introdução

O termo Cidade Inteligente (CI) é utilizado para representar o conceito da redução dos problemas resultantes da urbanização por meio da utilização de novas tecnologias, tornando o ambiente da cidade mais sustentável e eficiente (XIE *et al.*, 2019). Dentre as características de uma CI, podemos citar o uso pervasivo de Tecnologias de Informação e Comunicação (TIC) em diversos domínios urbanos para aumentar a eficiência na utilização de seus recursos (NEIROTTI *et al.*, 2014). Os domínios de aplicação em Cidades Inteligentes (CIs) são amplos e como exemplo podemos citar: redes de energia, transporte e mobilidade urbana, logística, saúde, segurança pública, administração pública e governança, ambiente e sustentabilidade, dentre outros. Dentre as tecnologias utilizadas em CIs podemos citar a IoT, que é utilizada principalmente para sensoriamento e atuação sobre o ambiente da cidade.

A IoT é um paradigma que reúne diversos conceitos e tecnologias, tais como computação ubíqua e pervasiva, e tecnologias de sensoriamento e comunicação. Dessa forma, dispositivos equipados com sensores e atuadores (e.g., *smartphones*) podem se interconectar de maneira que haja uma interação contínua entre o mundo real e o digital (BORGIA, 2014). Sistemas IoT permitem que objetos sejam capazes de interagir entre si, atuem de acordo com as suas interpretações e troquem informações com pessoas. Estes objetos, sendo físicos ou digitais, constituem a base da IoT e são chamados de Objetos Inteligentes (KORTUEM *et al.*, 2009).

No contexto de CIs a IoT se apresenta como tecnologia-chave pois, através dela, pode-se utilizar sensores e atuadores para coletar dados em tempo real e utilizar tais dados para tomada de decisões e atuação sobre o ambiente físico da cidade. Ao conectar os sensores e atuadores através de uma rede de comunicação torna-se possível desenvolver serviços e aplicações para monitorar e gerenciar o uso dos recursos da cidade em busca de um ambiente mais sustentável. Como exemplo de aplicação de uma CI, podemos considerar o cenário de uma ambulância do sistema de saúde pública de uma cidade. Esta ambulância é equipada com um dispositivo transmissor de suas coordenadas geográficas enquanto tais coordenadas são consumidas por um semáforo inteligente capaz de liberar as vias de trânsito ao receber notificações de proximidade da ambulância. Em outro exemplo, podemos ter uma viatura policial equipada com uma câmera de segurança e um dispositivo inteligente que transmite imagens das placas dos veículos observados para um sistema de monitoramento em tempo real cujo objetivo é identificar e gerar alertas para veículos em estado de infração.

Um dos grandes desafios envolvendo as CIs consiste na segurança da informação,

que aborda desde problemas relacionados à proteção de dados, assim como do software e também da infraestrutura utilizada para processar e armazenar os dados (ALAMER; ALMAIAH, 2021). As CIs também estão susceptíveis a ameaças de segurança tais como: negação de serviço, invenção e modificação de dados, acesso não autorizado a serviços e dados. Estas ameaças tem potencial para causar grandes prejuízos em uma cidade inteligente, de forma que a segurança computacional desempenha um papel crucial na proteção dos sistemas de informação e comunicação que sustentam as infraestruturas e serviços urbanos da cidade. Requisitos básicos de segurança como confidencialidade, integridade, irretratabilidade, disponibilidade, controle de acesso e privacidade também se aplicam às CIs e devem estar presentes no mundo físico (i.e., no sensoriamento), na comunicação e nas informações (ZHANG *et al.*, 2017).

Negligenciar a segurança no contexto de CIs pode resultar em consequências indesejadas, tais como: exposição de dados pessoais e sensíveis dos cidadãos; e interrupções significativas nos serviços essenciais, como transporte público, fornecimento de água, energia e serviços de emergência. Tais consequências também podem gerar falta de confiança do público em relação às tecnologias e serviços oferecidos pelas cidades, agravando ainda mais os problemas. O ambiente complexo e heterogêneo de uma CI, com diferentes atores, protocolos de comunicação e interações diversas dificulta a implementação de mecanismos de segurança. Portanto, é necessário que a segurança da informação seja uma prioridade em todas as etapas do desenvolvimento de soluções para CIs, desde especificação até a implantação.

Neste sentido, a Gestão de Identidades pode desempenhar um papel fundamental na garantia da segurança em ambientes de IoT e CI. Através da identificação de todos os atores existentes em uma CI torna-se possível implementar mecanismos de segurança capazes de assegurar a procedência dos dados provenientes do sensoriamento, controlar acesso aos dispositivos, serviços, aplicações e recursos da cidade, assim como garantir a integridade e confidencialidade de dados trafegados. Ao considerar a gestão de identidades aplicadas a uma CI, espera-se que seja possível desenvolver um ambiente propício para a identificação e gestão transparente e segura dos recursos da cidade, assim como dos atores que ali existem e que podem se comunicar, produzir e consumir dados. Como exemplo prático de atores existentes em uma CI, podemos citar órgãos públicos tais como prefeituras, sub-prefeituras, secretarias ou similares, pessoas, dispositivos IoT (i.e., sensores e atuadores), serviços, sistemas e aplicações. Um sistema de Gestão de Identidades voltado para CI, portanto, deve oferecer os meios para que sejam desenvolvidos mecanismos para estabelecimento de canais seguros de comunicação, autenticação e controle de acesso entre estes participantes, de forma transparente e auditável.

A tecnologia *blockchain* oferece uma forma inovadora de promover a confiança em sistemas digitais, eliminando a necessidade de confiança mútua entre os participantes. Com

o uso de registros distribuídos e imutáveis, as transações são verificadas e validadas por todos os nós da rede, garantindo integridade e segurança. Essa característica é particularmente valiosa para aplicações de IoT e CIs, onde dispositivos e sistemas interagem continuamente. Ao utilizar blockchain, é possível aumentar a confiabilidade das aplicações, pois os dados são registrados de forma transparente e resistente a alterações, proporcionando uma base segura para a troca de informações, mesmo que os dispositivos ou partes envolvidas não confiem umas nas outras.

Para melhor contextualização sobre a temática deste trabalho, toma-se como exemplo o cenário de uma CI administrada por entidades administrativas do poder público. Estas entidades desejam implantar dispositivos IoT (e.g., sensores, semáforos inteligentes, ambulâncias com *Global Positioning System* (GPS), câmeras de segurança, etc) para monitorar ou atuar sobre o ambiente da cidade. Em posse dos dados coletados pelo sensoriamento da cidade, os gestores da cidade podem tomar decisões baseadas em dados oriundos do sensoriamento e também desenvolver serviços e aplicações para atender as necessidades dos cidadãos. Sem a garantia da segurança e integridade dos dados provenientes do sensoriamento, torna-se inviável para a administração da cidade tomar decisões estratégicas, atuar sobre o ambiente da cidade ou disponibilizar tais dados para serviços e aplicações.

1.1 Contexto Geral

Em ambientes de IoT e CIs, os Sistemas de Gestão de Identidade desempenham um papel crucial na garantia da segurança e na proteção dos dados. Esses sistemas permitem a autenticação segura e o gerenciamento de acesso para uma ampla gama de atores, incluindo dispositivos IoT, gateways de comunicação, pessoas e serviços. Por meio da atribuição de identidades únicas e credenciais de acesso, os dispositivos podem ser autenticados e autorizados a se comunicar com outros dispositivos e sistemas existentes na infraestrutura da cidade. Além disso, os Sistemas de Gestão de Identidade permitem o controle preciso de quem tem acesso a quais dados e recursos, garantindo a segurança da informação. Isso inclui não apenas os dispositivos IoT, mas também as pessoas que interagem com esses dispositivos e os serviços e aplicações oferecidos pela cidade inteligente. Ao integrar todos esses atores em um sistema de Gestão de Identidade unificado, as CIs podem garantir a segurança e a confiabilidade de suas operações, promovendo assim um ambiente urbano seguro, transparente e auditável.

1.2 Caracterização do Problema

O principal problema abordado neste trabalho decorre do fato de que os sistemas tradicionais de Gestão de Identidade não foram projetados para lidar com cenários de CI.

Estes sistemas, geralmente centralizados, são mais propensos a sofrer com problemas de escalabilidade e apresentar pontos únicos de falha. Falhas de segurança e ataques cibernéticos em larga escala representam um risco significativo para a integridade dos dados e para a disponibilidade de serviços essenciais de uma CI. À medida que a rede de dispositivos IoT cresce, esses sistemas centralizados tornam-se cada vez mais sobrecarregados e ineficientes. Além disso, os diferentes atores que existem em uma cidade possuem suas especificidades, o que torna desafiador estabelecer mecanismos eficientes e seguros para a Gestão de Identidades. Nesta dissertação de mestrado, a tecnologia *blockchain* será utilizada como um meio para mitigar os problemas de centralização, e falta de transparência presentes nos Sistemas de Gestão de Identidade tradicionais e para propor um sistema de gestão de identidades transparente e flexível o bastante para aplicação em cenários de CI.

1.3 Objetivos

O objetivo geral desta pesquisa é propor um modelo de Gestão de Identidades para CIs, que será implementado em um ambiente descentralizado baseado em blockchain, e integrado a plataforma *InterSCity* [1] como prova de conceito. Dentre os objetivos específicos, tem-se:

- Propor um modelo para Gestão de Identidades, levando em conta os diferentes atores que existem e interagem em uma CI e seus relacionamentos;
- Implementar o modelo proposto, com operações de registro, autenticação e revogação de identidades, utilizando a tecnologia blockchain e contratos inteligentes;
- Integrar o modelo de Gestão de Identidades à plataforma *InterSCity*, para prover autenticação e controle de admissibilidade sobre os dispositivos IoT que inserem dados na plataforma;
- Avaliar a solução proposta fazendo uma análise acerca do custo computacional e aplicabilidade da solução proposta em ambientes de cidades inteligentes.

1.4 Organização do Trabalho

O restante desta dissertação está organizado da seguinte forma. O Capítulo 2 introduz conceitos importantes para o melhor entendimento desta dissertação. Neste capítulo serão apresentados os conceitos de Gestão de Identidades, assim como da tecnologia *Blockhain* e suas vantagens para o desenvolvimento de aplicações. O Capítulo 3 apresenta os trabalhos relacionados, no qual serão apresentados modelos similares a solução proposta

[1] https://interscity.org/software/interscity-platform/

e também será feita uma comparação entre os trabalhos apresentados e a solução proposta. O Capítulo 4 aborda a solução proposta assim como sua implementação e integração com uma plataforma de cidades inteligentes chamada *InterSCity* para prover uma infraestrutura de segurança para a plataforma. O Capítulo 5 apresenta uma avaliação sobre a solução proposta, aqui serão apresentados os custos computacionais ao adotar-se o modelo proposto e também será feita uma discussão a respeito da aplicabilidade do modelo em ambientes de IoT e CI. Por fim, o Capítulo 6 conclui o trabalho, retomando os objetivos iniciais e discutindo os resultados obtidos assim como as principais contribuições e perspectivas futuras deste trabalho.

2 Fundamentação Teórica

Nesta seção apresenta-se a fundamentação teórica na qual se baseia o desenvolvimento do trabalho. Serão apresentados os principais conceitos envolvidos tais como: Identidades e a Gestão de Identidades, assim como a tecnologia *blockchain*.

2.1 Identidades e Gestão de Identidades

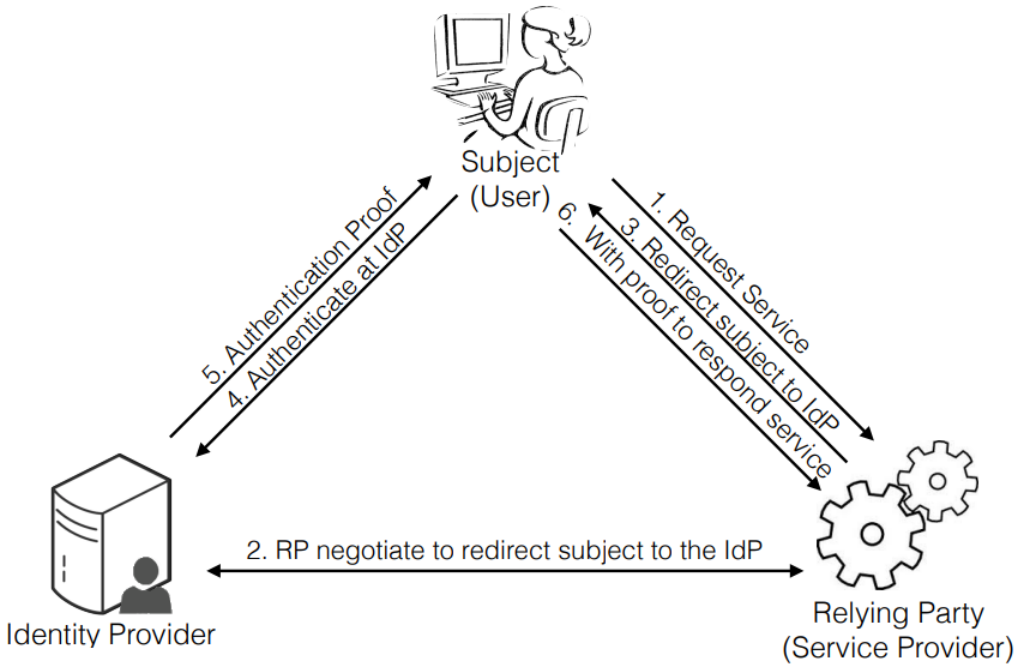
Identidades são popularmente conhecidas como "algo que identifica" e são utilizadas cotidianamente, como ao apresentar a habilitação para identificar-se e comprovar o direito de conduzir veículos. O conceito de identidade pode ser formalmente definido como a informação sobre uma entidade que é suficiente para identificá-la em um contexto específico (ITU, 2009). Além do conceito geral de identidade, também existe o conceito de identidade digital. Segundo (HADDOUTI; KETTANI, 2019), uma identidade digital refere-se a um conjunto de informações que identificam exclusivamente um indivíduo utilizando dados digitais para garantir o mesmo nível de confiança que uma transação presencial geraria. Segundo (MÜHLE *et al.*, 2018) uma identidade digital é um meio no qual pessoas podem provar eletronicamente que elas são quem dizem ser e se diferenciar uma das outras. O termo Gestão de Identidades é uma tradução do inglês para *Identity Management* (IdM), Como sinônimo também utiliza-se o termo Gestão de Identidade e Acesso ou *Identity and Access Management* (IAM). A Gestão de Identidades é uma linha de pesquisa com diversas aplicações relacionadas à segurança computacional.

Segundo (BERTINO; TAKAHASHI, 2010), a Gestão de Identidades pode ser definida como manter a integridade de identidades ao longo de seu ciclo de vida com objetivo de disponibilizar as identidades e seus dados relacionados para serviços de forma segura. Segundo a União Internacional de Telecomunicações (ITU) (ITU, 2009), a Gestão de Identidade se refere a gestão das informações contidas nas identidades através de operações como emissão, revogação, atualização e obtenção de identidades. Em (MANOHAR; BRIGGS, 2018), a Gestão de Identidades é uma diretriz de segurança que permite que os indivíduos certos acessem os recursos certos, no momento certo e por razões corretas. Segundo (LIU *et al.*, 2020), a Gestão de Identidades se refere a um arcabouço (i.e., *framework*) de políticas e tecnologias para garantir que apenas indivíduos autorizados acessem os recursos pertencentes a uma determinada organização.

Os conceitos apresentados reforçam que a Gestão de Identidades não envolve somente a manutenção (i.e., emissão, atualização, revogação, etc) de identidades, mas também mecanismos para autenticação e controle de acesso. Sistemas computacionais que efetuam a gestão das identidades são chamados de Sistemas de Gestão de Identidades, ou

Identity Management System (IdMS). Estes sistemas podem implementar diferentes tipos de arquiteturas com a finalidade de oferecer os meios para que serviços e aplicações possam operar de forma segura. Tradicionalmente, os IdMS adotam uma arquitetura centralizada, que envolve três atores principais: o Sujeito (usuário), o Provedor de Identidades e o Provedor de Serviço. A Figura 1 ilustra tais atores, e detalha um pouco sobre o funcionamento geral desses sistemas no qual um usuário tenta acessar algum serviço de um provedor de serviços.

Figura 1 – Atores de um Sistema de Gestão de Identidades Tradicional.



Fonte: (ZHU; BADR, 2018).

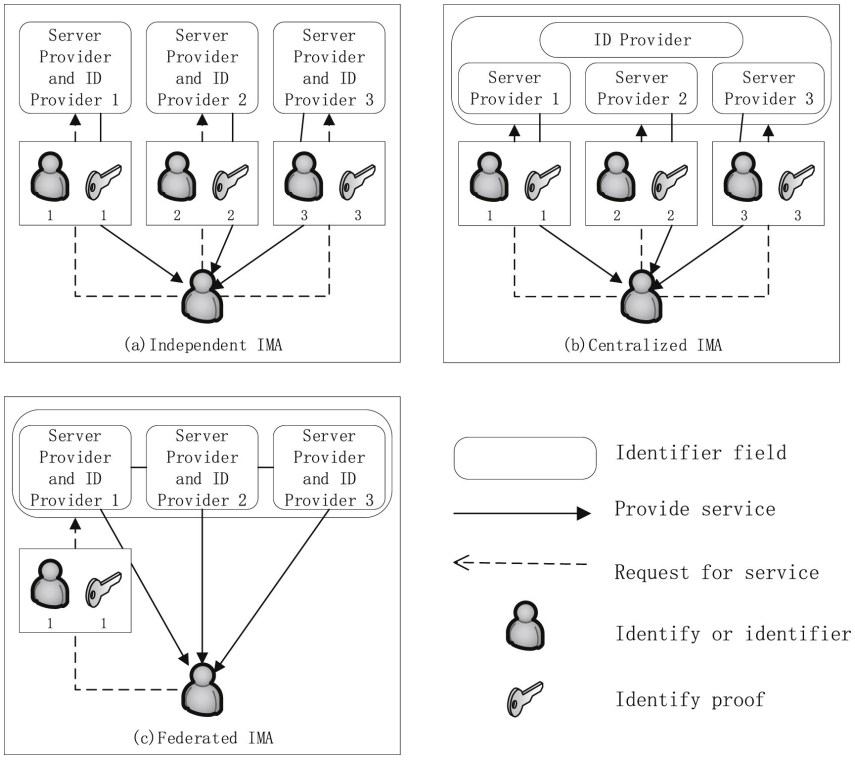
Neste exemplo o usuário (*subject*) inicialmente requisita algum serviço ao provedor de serviços (*service provider*) e após isso o provedor de serviços inicia a negociação com o provedor de identidades (*identity provider*) que então redireciona o usuário para que se autentique com o provedor de identidades. Após a autenticação ser concluída, o usuário em posse da prova de autenticação pode ser redirecionado para acessar o serviço desejado. Ressalta-se que os IdMS são responsáveis por manter as informações de identidade do usuário, tais como identificadores (e.g., nome de usuário, *e-mail*, etc), suas credenciais (e.g., certificados, *tokens*, etc) e seus atributos (e.g., papeis, posições e privilégios) (ZHU; BADR, 2018).

2.1.1 Arquiteturas para Gestão de Identidade

Em (LIU *et al.*, 2020), são apresentados três arquiteturas de gestão de identidades, que são: Independente, Centralizada e Federada. A Figura 2 ilustra estas três arquiteturas, na qual estão contidos os usuários, provedores de serviço, provedores de identidade,

identidades ou identificadores, e as credenciais. As setas pontilhadas representam uma requisição de serviço e as setas preenchidas a provisão do serviço.

Figura 2 – Arquiteturas para Gestão de Identidades: Independente, Centralizada e Federada.



Fonte: (LIU *et al.*, 2020).

Na Figura 2 (a) apresenta-se a arquitetura independente, no qual cada provedor de serviço também atua como provedor de identidade armazenando os dados de identidade de seus usuários. Dessa forma, as identidades de provedores de serviços diferentes não possuem interoperabilidade e um mesmo usuário precisaria manter suas informações de identidade e contas de usuário com cada provedor de serviço. Apesar desta arquitetura ser simples em termos de implementação ela não é escalável pois ao aumentar o número de provedores de serviço aumenta-se também os custos de armazenamento dos dados dos usuários que muitas vezes são redundantes. Além disso, este modelo não é vantajoso para o usuário, pois além de precisar manter várias contas diferentes a reutilização de senhas acaba sendo estimulada, o que pode aumentar a superfície de exposição dos dados pessoais e riscos de vazamento de dados. Na Figura 2 (b) apresenta-se a arquitetura centralizada, no qual existe apenas um provedor de identidade em um determinado domínio de confiança. Dessa forma, todos os provedores de serviço, no mesmo domínio de confiança, compartilham as identidades dos usuários. Uma arquitetura centralizada apresenta algumas desvantagens, como a existência de ponto único de falha, que pode comprometer os serviços de segurança de múltiplos provedores de serviço. Na Figura 2 (b) apresenta-se a arquitetura federada, existe a interconexão de múltiplos sistemas de gestão de identidades, que podem pertencer

a diferentes domínios. Ao possuir credenciais de um provedor de identidade pertencente a uma federação, o usuário pode acessar serviços de qualquer provedor de serviços que também faça parte da federação. Esta abordagem estimula a colaboração e também reduz a redundância dos dados uma vez que o usuário pode manter sua identidade com apenas um provedor de identidade e ainda assim ter acesso a todos os serviços.

Existem ainda arquiteturas híbridas, que combinam aspectos das arquiteturas apresentadas anteriormente, e também arquiteturas que são voltadas para proteção do usuário e de seus dados. Uma arquitetura centrada no usuário coloca o controle das identidades diretamente nas mãos dos próprios usuários. Nesta abordagem, os usuários têm autonomia para gerenciar suas próprias identidades e dados pessoais, decidindo quando e como compartilhar essas informações com diferentes provedores de serviços. Esta arquitetura é frequentemente implementada através de tecnologias como *Self-Sovereign Identity* (SSI), ou Identidades Auto-soberanas. O termo SSI, em essência, refere-se a um sistema de gestão de identidades que permite que indivíduos possuam e gerenciem completamente sua identidade digital (MÜHLE *et al.*, 2018). Seu propósito é aumentar a confiança e segurança, enquanto preserva a privacidade do usuário e protege o mesmo do constante aumento de controle central por parte de terceiros, em outras palavras, usuários são soberanos de si e possuem total controle sobre sua identidade (HADDOUTI; KETTANI, 2019).

2.2 A Tecnologia *Blockchain*

A tecnologia *blockchain* popularizou-se em 2008, após a publicação de um artigo técnico de título "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (NAKAMOTO, 2008). O autor, utilizando o pseudônimo *Satoshi Nakamoto*, apresenta uma implementação de uma *blockchain* que funciona como um livro-razão público e distribuído para registrar todas as transações de uma criptomoeda chamada *Bitcoin*. Uma *blockchain* é essencialmente um livro-razão descentralizado, distribuído, compartilhado e imutável que armazena registros de ativos e transações através de uma rede peer-to-peer (KHAN; SALAH, 2018). O termo *Distributed Ledger Technology* (DLT), ou livro-razão distribuído, é o conceito utilizado na *blockchain* que consiste em uma cadeia ordenada e consistente de transações distribuída em diversos nós de uma rede Peer-to-Peer[1] (Conceição; Rocha, 2020). As definições de *blockchain* variam conforme os autores, apesar disso todas são similares. Em (XIE *et al.*, 2019) a *blockchain* é descrita como um banco de dados compartilhado, imutável, descentralizado, e disponível publicamente, onde todas as transações são armazenadas e qualquer pessoa nesse sistema pode acessar, enviar e verificar transações. A tecnologia *blockchain* foi prevista pela indústria e pela comunidade acadêmica como sendo uma tecnologia disruptiva

[1] ponto a ponto

que é adequada para desempenhar um papel fundamental no gerenciamento, controle e principalmente na proteção de dispositivos IoT (KHAN; SALAH, 2018).

2.2.1 Características da *Blockchain*

A tecnologia *blockchain* oferece diversas vantagens no desenvolvimento de aplicações, tais como descentralização da informação, disponibilidade, privacidade, integridade, imutabilidade e auditabilidade (Conceição; Rocha, 2020). Tais características tornam a *blockchain* uma boa escolha para um conjunto de aplicações, sobretudo aquelas que exigem maior segurança e transparência como é o caso de aplicações voltadas para o domínio das Cidades Inteligentes.

A descentralização da informação é capaz de eliminar a necessidade de uma autoridade central e também de intermediários. Ao distribuir os dados através de uma rede de nós, a rede como um todo torna-se mais resistente contra falhas pontuais e ataques. Também garante-se maior disponibilidade para os dados e aplicações construídas utilizando à *blockchain*. Tais características são fundamentais para sistemas que necessitam de alta disponibilidade. A privacidade é uma propriedade que pode ser explorada, uma vez que muitas *blockchains* utilizam mecanismos criptográficos para oferecer transações anônimas, oferecendo mais proteção para os usuários da rede.

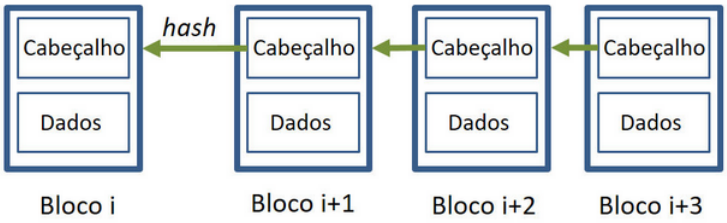
A integridade dos dados é naturalmente suportada nas *blockchains* nas quais existem mecanismos baseados em criptografia para garantir que o dado não pode ser alterado uma vez que é inserido na cadeia de blocos. Esta propriedade é fundamental em contextos em que a confiança nos dados é requerida. Além disso a imutabilidade garante que os dados inseridos não possam ser excluídos, criando-se assim registros históricos sólidos, transparentes e auditáveis. Todas as transações efetuadas a rede *blockchain* podem ser verificadas, de forma que a auditabilidade também é uma propriedade chave para aumentar a confiança nos sistemas e aplicações baseadas em *blockchain*.

2.2.2 Funcionamento

A Figura 3 ilustra a estrutura na qual os dados são armazenados na *blockchain*. A *blockchain*, ou cadeia de blocos, possui uma estrutura encadeada na qual blocos com dados são registrados de forma conectada ao bloco anterior. Nesta estrutura de blocos encadeados cada bloco é composto por um conjunto de transações e cada bloco possui um resumo *hash* do bloco anterior que é utilizado para manter a integridade da cadeia na medida que ela cresce. Como a *blockchain* executa em uma rede *Peer-to-Peer* é necessário utilizar algoritmos de consenso para que os participantes consigam entrar em comum acordo a respeito de qual participante terá direito a propor o novo bloco. O consenso é o processo pelo qual, a partir de um grupo de participantes independentes, todos os

participantes corretos atingem a mesma decisão coletiva de aceitar o novo bloco a ser inserido na corrente de blocos (REBELLO *et al.*, 2019). Como resultado prático garante-se que os mesmos blocos sejam inseridos na mesma ordem em todos os nós.

Figura 3 – Estrutura básica de uma *blockchain*.



Fonte: (Conceição; Rocha, 2020).

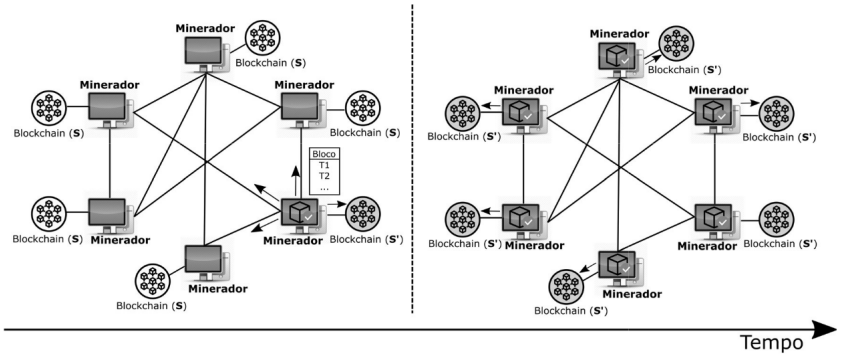
A integridade dos dados registrados nos blocos é garantida a medida que a cadeia cresce, tornando assim impraticável alterar um dado de uma *blockchain* sem alterar a cadeia inteira. A estrutura em cadeia da *blockchain* com cada bloco contendo o resumo *hash* do bloco anterior garante que para alterar algum dado seria necessário alterar os *hashs* de todos os blocos da cadeia. Para alterar toda a cadeia de blocos seria necessário dedicar um imenso poder computacional e caso um dado fosse alterado sem alterar a cadeira inteiramente isso seria facilmente percebido através dos resumos *hash*.

A Figura 4 ilustra o processo de atualização do estado de uma *blockchain*, isto é feito a partir de um processo chamado mineração. A mineração é o processo no qual é feito a escolha de qual nó participante tem o direito de propor a inclusão do próximo bloco. Após essa escolha o participante propõe o bloco que então é validado pelos demais participantes antes de ser inserido na rede. Os mineradores são participantes da rede que competem para resolver um problema matemático complexo, que exige um grande poder computacional. O primeiro minerador a resolver o problema tem direito de incluir o próximo bloco na rede, e os demais mineradores verificam a validade do bloco antes de inseri-lo. Após a adição do bloco na rede, são geradas criptomoedas para o minerador, como forma de recompensa-lo pelo trabalho. Este processo não é algo genérico para qualquer rede *blockchain*, ele se chama prova de trabalho, e nada mais é do que um algoritmo de consenso executado entre os mineradores de uma rede *blockchain*.

2.2.3 Principais Algoritmos de Consenso

Algoritmos de consenso são mecanismos utilizados em sistemas distribuídos para garantir que os sistemas participantes consigam negociar para chegar a um entendimento ou acordo comum antes de tomar ações específicas (SINGHAI, 2008). No caso da *blockchain*, esse acordo comum consiste em qual bloco deve ser inserido na rede, decisão esta que deve ser cumprida por todos os nós participantes da rede. Em outras palavras, o consenso

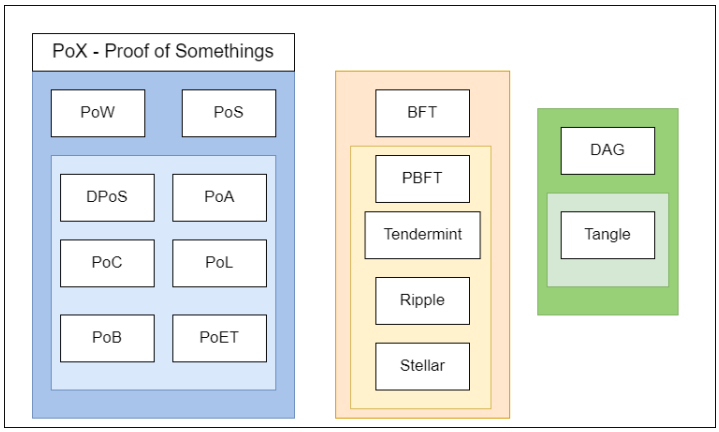
Figura 4 – Atualização do estado de uma *blockchain*.



Fonte: (REBELLO *et al.*, 2019).

consiste em uma decisão unânime e irrevogável a partir de um conjunto de valores propostos em uma rede (MACEDO, 2011). Esses algoritmos são fundamentais para manter a integridade e a segurança da rede *blockchain*, garantindo que todos os participantes tenham uma cópia sincronizada do livro-razão. A Figura 5 ilustra alguns dos principais algoritmos de consensos utilizados em *blockchains*. Em seguida, resumiremos os principais algoritmos de consenso. Existem basicamente duas classificações de algoritmos de consenso, os probabilísticos e os determinísticos. Nos algoritmos de consenso probabilísticos, como o nome sugere, baseiam-se em uma probabilidade para alcançar o consenso. Isso significa que eles não garantem um consenso absoluto, mas oferecem uma alta probabilidade de acordo entre os participantes.

Figura 5 – Principais algoritmos de consenso em *blockchains*.



Adaptado de: (FABIOLA, 2021).

Na *Proof of Work* (PoW), ou Prova de Trabalho, os nós da rede, ou mineradores, competem para resolver um problema matemático complexo. O primeiro nó a resolver o problema ganha o direito de inserir o próximo bloco de transações na rede *blockchain* e assim receber uma recompensa pelo trabalho realizado. Este processo demanda grande quantidade de poder computacional e possui alto gasto de energia, não sendo considerável

ecologicamente sustentável. Apesar disso, a grande quantidade de poder computacional necessária para propor os próximos blocos torna mais difícil que nós maliciosos tentem alterar o estado da rede, pois, para isso, seria necessário possuir metade do poder computacional aplicado a rede. O *Bitcoin* é um exemplo de *blockchain* que utiliza PoW.

Na *Proof of Stake* (PoS), ou Prova de Posse, os nós que propõem blocos são chamados de validadores, e estes são selecionados com base na quantidade de recursos (i.e., criptomoeda) que possuem. Quanto maior a quantidade de moedas que o nó possui, maior a probabilidade de que este nó seja o escolhido para validar o próximo bloco a ser inserido na rede *blockchain*. Caso um nó aja de forma maliciosa, ele pode perder seus recursos. A Prova de Posse é mais eficiente que a Prova de Trabalho em termos de consumo de energia. Em 2022 a plataforma Ethereum [2] adotou oficialmente a prova de posse, deixando assim de usar a prova de trabalho. A *Delegated Proof of Stake* (DPoS), ou Prova de Posse Delegada, funciona de maneira similar a PoS, porém aqui os participantes que detêm recursos possuem votos para eleger um delegado que será o responsável por validar transações e adicionar os blocos à rede *blockchain*. Quanto mais recursos um participante possui, mais votos ele tem disponível para exercer. Este mecanismo é mais rápido e eficiente que o PoS, pois reduz o número de nós que participam diretamente no processo de validação de transações. Como exemplo de *blockchain* que utiliza este algoritmo, tem-se a EOS [3].

Na *Proof of Authority* (PoA), ou Prova de Autoridade, um número limitado de validadores confiáveis é previamente selecionado, estes tornam pública sua identidade e reputação como forma de aumentar a transparência. Estes validadores têm autonomia para criar novos blocos e validar transações. Este modelo é menos centralizado, porém mais eficiente. Sua utilização ocorre mais frequentemente em *blockchains* privadas ou de consórcio. Como exemplo, tem-se a VeChain [4].

Na *Proof of Burn* (PoB), ou Prova de Queima, os participantes da rede destroem determinada quantidade de recursos (i.e., criptomoeda), transferindo tais recursos para um endereço irrecuperável. Como troca por tal queima de recursos, os nós recebem a oportunidade de minerar novos blocos de forma proporcional ao valor destruído. Este algoritmo tem como intenção simular os custos de *hardware* da prova de trabalho, porém sem o consumo de energia gasto para resolver os desafios matemáticos.

Na *Proof of Capacity* (PoC), também conhecida como Prova de Capacidade, os mineradores precisam alocar espaço de armazenamento em disco para poder participar do processo de validação de blocos. Quando maior o espaço alocado, maior é a chance do minerador ser o participante escolhido para propor o próximo bloco à *blockchain*. Como exemplo de criptomoeda que utiliza este algoritmo, tem-se a *Burstcoin* [5]

[2] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
[3] https://eosnetwork.com/
[4] https://vechain.org/
[5] https://burstcoin.info/

Existem ainda algoritmos de consenso que são baseados em *Byzantine Fault Tolerance* (BFT), ou Tolerância a Falhas Bizantinas, esta abordagem permite a presença de alguns nós maliciosos ou falhos, desde que esse número não ultrapasse determinado limite (dois terços de nós honestos). A implementação mais conhecida é *Practical Byzantine Fault Tolerance* (PBFT), que é utilizada por *blockchains* como *Hyperledger Fabric*[6].

As *blockchains Directed Acyclic Graph* (DAG) são uma variação das *blockchains* tradicionais que exploram o paralelismo no sistema tradicional de blockchain de cadeia única e utilizam uma estrutura de dados de grafo direcionado acíclico para conectar blocos (FABIOLA, 2021). O mecanismo de consenso, diferenciado dos abordados anteriormente, faz com que cada transação seja ligada a dois registros de transações anteriores através do grafo. Isso permite que múltiplas transações sejam processadas simultaneamente, aumentando a escalabilidade e reduzindo a latência das transações. Em um DAG, cada nova transação referencia transações anteriores, eliminando a necessidade de mineração e reduzindo o consumo de energia. Como exemplo de rede *blockchain* que utiliza DAG temos a *IOTA* [7].

2.2.4 Comparativo Entre os Algoritmos de consenso

Os algoritmos de consenso "Proof of Something"(PoW, PoS, DPoS), BFT e DAG representam abordagens distintas para alcançar consenso em sistemas distribuídos e *blockchains*, cada um com suas vantagens e desvantagens específicas. A PoW por exemplo, é utilizada na *bitcoin* para garantir a segurança, porém a um alto custo de energia elétrica. Já a PoS oferece eficiência energética ao selecionar validadores com base na quantidade de moedas apostadas. Os BFT concentram-se em garantir o correto funcionamento do sistema mesmo na presença de nós maliciosos. Por outro lado, os algoritmos DAG utilizam uma estrutura de grafo direcionado sem ciclos, oferecendo alta escalabilidade e flexibilidade, este modelo é ideal para aplicações com alta taxa de transações e microtransações. Em resumo, enquanto PoW e PoS oferecem uma troca entre segurança e eficiência energética, BFT garante robustez contra falhas bizantinas em redes com participantes pré-determinados.

A Tabela 1 apresenta uma comparação entre os principais algoritmos de consenso. Observa-se a partir da tabela, que os algoritmos do tipo prova de alguma coisa são resistentes a falhas bizantinas ou de parada em até metade de seus participantes, e que a confirmação das transações geralmente ocorrem em um tempo mais alto, acima de 100 segundos, também nota-se que o número de transações por segundo fica abaixo de 100. Apesar destas taxas serem baixas, estes algoritmos são capazes de suportar um número mais elevado de participantes, onde o consenso ocorre probabilisticamente ao longo do tempo. Já os algoritmos baseados em BFT conseguem tolerar apenas 33% dos nós em falha,

[6] https://www.hyperledger.org/projects/fabric
[7] https://www.iota.org/

apesar disso a confirmação da transação nestes algoritmos de consenso determinísticos tende a ser muito menos, ocorrendo em até 10 segundos. Da mesma forma a taxa de transações por segundo é significativamente maior, porém nestes modelos o número de nós participantes são consegue escalar tão bem. Tais diferenças devem ser levadas em conta para a escolha da *blockchain* mais adequada ao contexto de negócio a qual deseja-se aplica-la.

Tabela 1 – Comparação entre algoritmos de consenso.

Características	**PoW**	**PoS**	**DPoS**	**PBFT**
Tolerância a falhas bizantinas	50%	50%	50%	33%
Tolerância a falhas de parada	50%	50%	50%	33%
Confirmação da transação	>100s	<100s	<100s	<10s
Transações por segundo	<100	<1000	<1000	<2000
Escalabilidade	Forte	Forte	Forte	Fraca

Fonte: (MINGXIAO *et al.*, 2017)..

2.2.5 *Blockchain* 2.0

O termo *blockchain 2.0* se refere à evolução da tecnologia *blockchain*, que, além de servir para o desenvolvimento de criptomoedas, passa a ser capaz de armazenar códigos (i.e., Contratos Inteligentes) na rede que podem ser utilizados para desenvolver aplicações descentralizadas. Em 2013, a plataforma *Ethereum* trouxe uma inovação ao permitir que programas de computador possam ser armazenados e executados na *blockchain* (QUEIROZ, 2018). Apesar disso, esta ideia já havia sido levantada anteriormente em 1997 por *Nick Szabo* ao propor um protocolo (SZABO, 1997) de transação informatizado que executa os termos de um contrato.

2.2.6 Contratos Inteligentes

Os contratos inteligentes são programas autoexecutáveis que ativam os termos e condições de um acordo ou contrato específico usando códigos de software e infraestrutura computacional (HEWA; YLIANTTILA; LIYANAGE, 2021). Como um programa em execução em uma *blockchain*, um contrato inteligente pode ser executado corretamente por uma rede de nós que não tem confiança entre si sem a necessidade de uma autoridade externa confiável, a natureza autoexecutável dos contratos inteligentes oferece oportunidade para uso em muitos campos que dependem de dados para conduzir transações (ZOU *et al.*, 2021). O uso de contratos inteligentes por parte de aplicações tem diversas vantagens, tais como: eliminação de intermediários, resistência a fraude, maior transparência, execução autônoma, e maior precisão ou capacidade de eliminação de vieses. Os contratos inteligentes poder ser explorados em diversas áreas, tais como: Saúde Pública, Logística, Finanças Descentralizadas, etc.

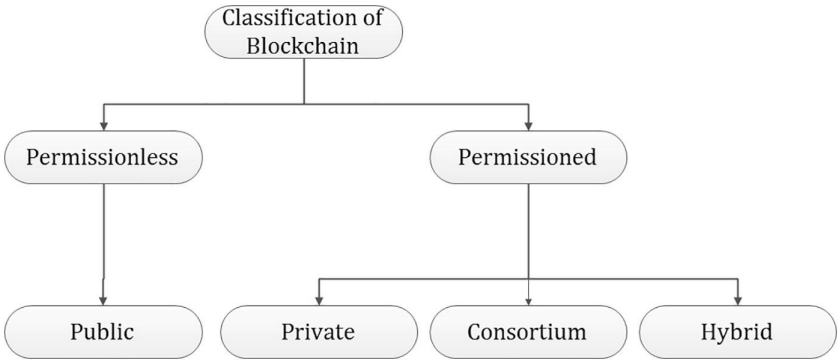
Na gestão de identidade, contratos inteligentes podem gerenciar identidades digitais verificadas e proteger informações pessoais, permitindo que os usuários controlem quem tem acesso aos seus dados. Eles também são utilizados para autenticação segura e descentralizada, eliminando a necessidade de serviços de autenticação centralizados. No setor imobiliário, os contratos inteligentes automatizam a transferência de títulos de propriedade e o registro de bens imóveis em uma blockchain. Além disso, podem automatizar pagamentos de aluguel e manter registros de contratos de locação, simplificando a administração de propriedades. Na cadeia de suprimentos e logística, os contratos inteligentes ajudam a rastrear a origem e o movimento de produtos, garantindo transparência e autenticidade. Pagamentos automáticos podem ser feitos quando mercadorias são entregues, com base em condições predefinidas, melhorando a eficiência do processo logístico. No setor de seguros, os contratos inteligentes permitem a criação de seguros no qual os pagamentos são feitos automaticamente com base em eventos predefinidos, como desastres naturais, sem a necessidade de processamento manual de sinistros. Eles também podem automatizar processos de apólices de seguros, desde a emissão até a renovação e pagamento de sinistros. Para votação e governança, os contratos inteligentes podem ser utilizados para criar sistemas de votação seguros e transparentes, registrando votos em uma blockchain. Eles também são usados no gerenciamento de decisões e processos de governança em organizações descentralizadas. No campo da propriedade intelectual e direitos autorais, os contratos inteligentes automatizam o licenciamento e pagamento de *royalties* para criadores de conteúdo. Além disso, monitoram e rastreiam o uso de obras protegidas por direitos autorais, garantindo que os criadores recebam o que lhes é devido. Os contratos inteligentes têm o potencial de revolucionar muitas indústrias ao automatizar processos, reduzir custos e aumentar a transparência e a segurança. Sua aplicação em diferentes setores demonstra a versatilidade e o impacto significativo que podem ter na forma como as transações e operações são conduzidas no mundo digital.

2.2.7 Tipos de *Blockchain*

As *blockchains* podem ser classificadas em permissionadas e não permissionadas. A Figura 6 ilustra os diferentes tipos de *blockchains* existentes dentro desta classificação: públicas, privadas, de consórcio e híbrida. As *blockchains* públicas, como *Bitcoin* e *Ethereum*, são descentralizadas e públicas no sentido de que qualquer um pode participar da rede, seja propondo ou validando novos blocos, ou mantendo cópias do *ledger*.

Neste tipo de *blockchain* geralmente emprega-se mecanismos de consenso probabilísticos, tais como a Prova de Trabalho, ou demais algoritmos chamados de “Prova de Alguma Coisa”. Como qualquer um pode unir-se a rede pública, o número de participantes tende a ser maior e consequentemente o tempo para atingir o consenso em *blockchains* públicas tende a ser maior do que as *blockchains* privadas.

Figura 6 – Tipos de *blockchain*.



Fonte: (RAJASEKARAN; AZEES; AL-TURJMAN, 2022).

Em contraste, as *blockchains* privadas, ou permissionadas, são controladas por uma única entidade, onde apenas participantes autorizados podem acessar e validar transações. Esse tipo é frequentemente utilizado na iniciativa privada que deseja manter um controle maior e mais privado sobre seus dados. Em *blockchains* privadas, os validadores da rede geralmente já se conhecem, e portanto pode-se adotar protocolos de consenso determinísticos, que chegam ao consenso em menos tempo.

As *blockchains* de consórcio, ou federadas, são geridas por um grupo de organizações confiáveis, que dividem o controle sobre a rede. Este tipo de *blockchain* pode ser explorado por indústrias, onde várias entidades ou *stakeholders* participam de forma colaborativa. Este modelo proporciona maior flexibilidade, pois permite que organizações mantenham a transparência e ao mesmo tempo proteja informações sensíveis. Como exemplo de áreas de aplicações de *blockchains* de consórcio, podemos citar aplicações de redes financeiras, ou rastreamento de cadeias de suprimento. Existem ainda *blockchains* híbridas, que podem combinar características de *blockchains* públicas e privadas, para oferecer maior flexibilidade e atender assim alguma regra de negócio específica. Cada tipo de *blockchain* oferece suas vantagens, e a sua escolha varia conforme as necessidades e casos de uso.

2.2.8 Aplicações de *blockchain* no Gerenciamento de Identidades

As características da *blockchain* são particularmente benéficas no contexto da CIs em que a segurança, transparência, integridade e auditabilidade dos dados e operações realizadas são cruciais para proteção dos recursos e dos cidadãos. Por isso, a *blockchain* vem sendo cada vez mais explorada nesse domínio. Na literatura, diversos autores exploram a tecnologia *blockchain* para aplicá-la no Gerenciamento de Identidade (GHAFFARI *et al.*, 2022). De acordo com (DUNPHY; PETITCOLAS, 2018), as tecnologias de *ledger* distribuído (e.g., *blockchains*) são adequadas para garantir consenso, transparência e integridade de transações efetuadas, e trazem diversos benefícios do uso de DLT aplicado a gestão de identidades, tais como: descentralização, imutabilidade, eficiência de custo e

disponibilidade.

A solução proposta nesta dissertação busca explorar a tecnologia *blockchain* e seus benefícios para conceber um modelo descentralizado de gestão de identidade para ambientes de CI. Através do uso da tecnologia *blockchain* para armazenar identidades digitais, é possível criar um ambiente democrático, seguro e transparente onde os participantes (i.e., entidades administrativas do poder público) podem compartilhar a mesma cadeia de blocos para gerenciar identidades de forma independente uns dos outros. Ao mesmo tempo, ao armazenar as identidades em uma rede *blockchain*, tem-se garantido um histórico imutável de todas as operações efetuadas e uma provisão íntegra das identidades que pode ser utilizada para fins de validação e auditoria das operações. O uso de *blockchain* para propor um modelo de gestão de identidades descentralizado inclui diversas vantagens em relação aos sistemas tradicionais, sendo um modelo mais adequado para aplicação em ambientes de CI.

3 Trabalhos Relacionados

Esta capítulo se dedica a compreender o estado da arte da gestão de identidade baseada em blockchain e voltada para IoT e CI. Inicialmente será apresentada a metodologia utilizada para a seleção dos trabalhos relacionados e em seguida serão resumidos aqueles trabalhos que se destacam por possuir características próximas da solução proposta nesta dissertação. Por fim, apresenta-se um quadro comparativo e conduz-se uma discussão em relação aos trabalhos.

3.1 Metodologia para Seleção dos Trabalhos Relacionados

Os trabalhos relacionados foram retirados de uma revisão da literatura já existente (AHMED *et al.*, 2022) que trata sobre sistemas de gestão de identidades baseados em *blockchain* e no ecossistema de identidades auto-soberanas. Esta revisão foi obtida a partir de buscas nas principais bases de dados de artigos científicos, especificamente: *Association for Computing Machinery* (ACM), *Institute of Electrical and Electronics Engineers* (IEEE), `Google Scholar`. A seguinte consulta foi utilizada para as buscas: ("Identity Management") AND ("IoT" OR "Smart Cities") AND ("Blockchain" OR "Blockchain based") AND ("Survey" OR "Literature Review" OR "Review"). Dentre os trabalhos obtidos nessa consulta, escolheu-se o mais completo. A seguir apresentaremos a revisão bibliográfica selecionada e posteriormente serão resumidos aqueles trabalhos que mais se aproximam da solução proposta.

3.2 *Blockchain-based Identity Management System and Self-sovereign Identity Ecosystem: A comprehensive Survey*

Em seu trabalho, (AHMED *et al.*, 2022) conduz uma revisão bibliográfica com foco nos sistemas de gestão de identidades baseados em *blockchain* e no ecossistema de identidades auto-soberanas. O artigo, apresenta uma extensa revisão da literatura sobre publicações acadêmicas e sobre soluções empresariais no que diz respeito à aplicabilidade de soluções de SSI baseadas em blockchain. A revisão também fornece uma visão detalhada dos elementos fundamentais da tecnologia blockchain e um *roadmap* progressivo das soluções de IdMS. Os trabalhos apresentados por esta revisão são classificados de acordo com a seguinte taxonomia: soluções de IdMS existentes no mercado, e soluções de IdMS baseadas em *blockchain* propostas ta literatura acadêmica. No primeiro caso, são apresentadas as principais plataformas de IdMS baseadas em *blockchain* assim como plataformas de IdMS não baseadas em *blockchain*. Em relação as soluções de IdMS baseadas em blockchain

propostas na literatura acadêmica, são apresentados trabalhos que subdividem-se nos seguintes domínios: computação em nuvem - *cloud computing*, IoT, redes de sensores sem Fio - *Wireless Sensor Network* (WSN) e soluções de IdMS genéricas. Aqueles trabalhos de IdMS inclusos no domínio da IoT possuem suas especificidades e podem abordar diferentes escopos. Os trabalhos são classificados ainda segundo os seguintes escopos:

- Modelo de confiança;
- Preservação de privacidade;
- Gestão de Identidades;
- Autenticação;
- Controle de acesso;

A partir dos trabalhos levantados nesta revisão bibliográfica, especificamente as soluções de IdMS, baseadas em blockchain, propostas na literatura acadêmica sobre a temática IoT foi possível encontrar aqueles trabalhos que são similares a solução proposta nesta dissertação. Os trabalhos que têm como escopo a Gestão de Identidades e Autenticação foram os mais próximos à solução apresentada nesta dissertação.

3.3 Resumo dos Trabalhos Relacionados

A seguir, serão resumidos os trabalhos relacionados. Para facilitar possíveis buscas optou-se por não traduzir os títulos dos trabalhos.

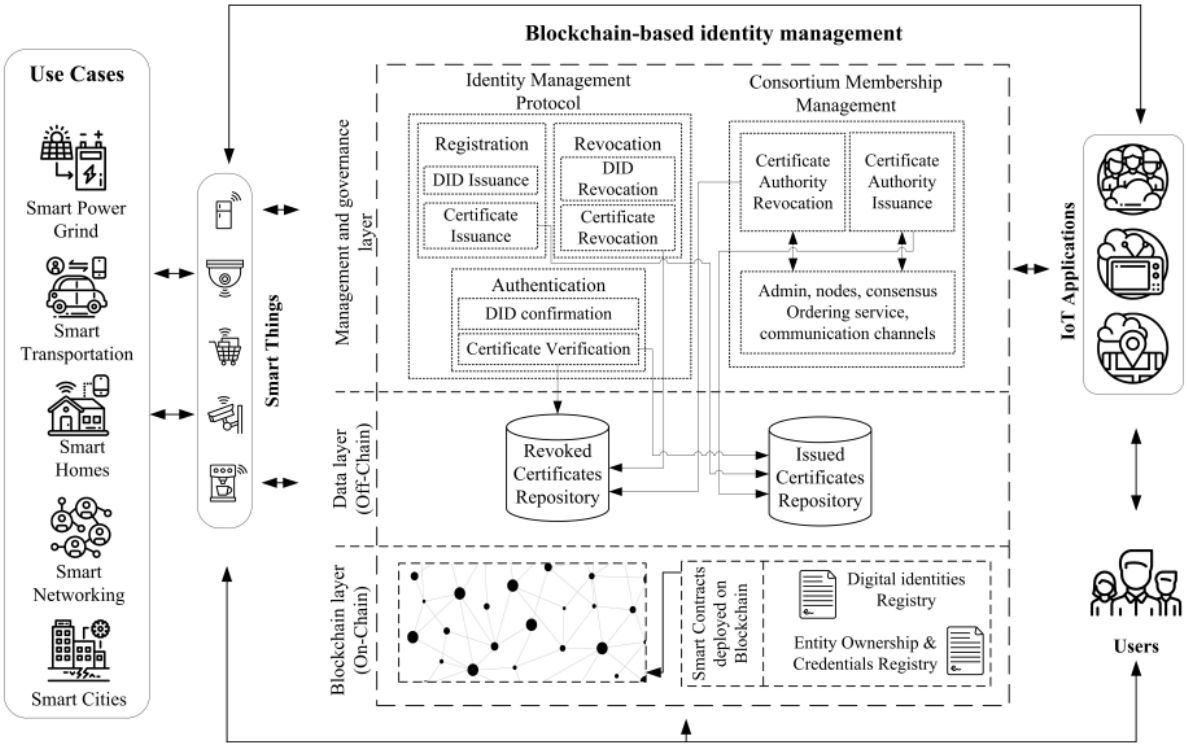
3.3.1 *A Lightweight Blockchain-Based IoT Identity Management Approach*

Em seu trabalho, (BOURAS *et al.*, 2021) tem como objetivo propor uma abordagem leve baseada em blockchain para a gestão de identidade voltada para Internet das Coisas. O autor considera que a gestão de identidades de dispositivos é um requisito fundamental para IoT. Sua motivação reside no fato de que soluções convencionais de gestão de identidade adotam arquiteturas centralizadas que podem levar a problemas como governança centralizada e pontos únicos de falha. Além disso, também são ponderadas questões de escalabilidade que são essenciais para ambientes IoT.

O modelo de gestão de identidades apresentado pelo autor, considera os seguintes atores existentes em ambientes de IoT: objetos inteligentes, aplicações IoT e usuários. E também leva em consideração os relacionamentos entre as diferentes entidades, pois as interações e trocas de dados na IoT podem ocorrer entre humano-dispositivo, dispositivo-dispositivo e dispositivo-aplicação. A Figura 7, ilustra a arquitetura geral da solução

proposta. Segundo a arquitetura, todos os atores que interagem no ecossistema da IoT, como usuários, dispositivos inteligentes e aplicativos, devem se registrar e autenticar na IdM baseada em blockchain. A rede blockchain atua como a espinha dorsal do ecossistema IoT, que é formada por um consórcio de organizações predefinidas que compartilha as mesmas necessidades industriais ou interesses comerciais e é responsável por construir e definir as políticas de rede e governar o ecossistema compartilhado. Para implementação desta arquitetura, utilizou-se o `Hyperledger Fabric`, onde foram escritos os contratos inteligentes que regem os protocolos para gestão das identidades. Os protocolos consistem em registro, autenticação e revogação de identidades. Para melhorar a escalabilidade e permitir que estas operações sejam feitas simultaneamente, foram utilizados três *ledgers* imutáveis, um para cada protocolo.

Figura 7 – Arquitetura geral da solução e interações.



Fonte: (BOURAS *et al.*, 2021)

Na blockchain, cada bloco contém um conjunto de transações de identidade emitidas pelo protocolo de identidade. Além da descentralização, privacidade e segurança oferecidas pela tecnologia de registro distribuído, o modelo proposto foi pensado para fornecer um protocolo simples e eficiente para atender às necessidades de todas as organizações de IoT. Em sua experimentação, é avaliada a eficácia da divisão das principais funcionalidades de um sistema de gestão de identidade em *ledgers* imutáveis separados. Para isso, envia-se uma série de requisições de registro, autenticação e revogação e avalia-se o tempo de resposta e mede-se o número de transações por segundo.

3.3.2 *Identity Management in IoT Networks Using Blockchain and Smart Contracts*

Em seu trabalho, (OMAR; BASIR, 2018) propõe a utilização da tecnologia blockchain para gestão de identidades voltada para Internet das Coisas IoT, visando estabelecer uma identidade digital única e global que possa ser mantida ao longo do ciclo de vida dos dispositivos de IoT. Além disso, sua solução também aborda os mecanismos para gestão da posse dos dispositivos (i.e, proprietários dos dispositivos) e atualizações de identidade. O autor utiliza a *blockchain* juntamente com criptografia de chave pública para identificação dos atores. A gestão de identidades é feita através de um livro-razão imutável e contratos inteligentes para implementação das regras e operações de identidade.

Segundo o autor, em ambientes IoT existe a necessidade de garantir-se a autenticação e autorização de dispositivos IoT de forma contínua, mesmo quando esses dispositivos estão conectados de forma intermitente ou temporária. Também existem diversos tipos de interação tais como humano-dispositivo, dispositivo-dispositivo ou dispositivo-serviços. Para isso é necessário que a autenticação e autorização dos dispositivos seja feita de forma bem definida por um sistema de gestão de identidades. Sua motivação, baseia-se no fato de que estas especificidades dificultam a aplicação dos sistemas tradicionais de gestão de identidades. Para que a comunicação entre esses dispositivos seja iniciada de forma segura, é essencial que haja um ciclo de vida bem definido para a gestão de identidade e que exista também um mecanismo de identificação único e global.

O modelo proposto pelo autor é baseado em três princípios: identidade como um ativo vivo (i.e., as identidades são atribuídas no nascimento do dispositivo), identidades são globais e únicas, e descentralização da autoridade. Suas principais contribuições consistem em: (I) propor mecanismo para gerar identificador global para dispositivos IoT, (II) modelar o ciclo de vida de uma identidade, (III) definir um processo de registro de identidades de dispositivos, (IV) prover meios para lidar com transferências de posse de dispositivos e (V) prover um mecanismo para rastreabilidade do ciclo de vida de um dispositivo ate sua origem.

Todas as operações são implementadas através de dois contratos inteligentes. Um é responsável por manter o registro de entidades com autorização de acesso para criar e atualizar as identidades digitais. O segundo contrato trata das funções de criação de identidade, transferência de identidade e verificação de identidade. Cada identidade de dispositivo é composta por um conjunto mínimo de atributos, tais como: número de série, nome do fabricante ou outros identificadores como endereço Media Access Control (MAC) ou Internet Protocol (IP). O processo de registro de identidades baseia-se fortemente em criptografia de chave publica e funções de *hash* para gerar os identificadores globais.

Em resumo, o autor apresenta uma abordagem descentralizada para gestão de

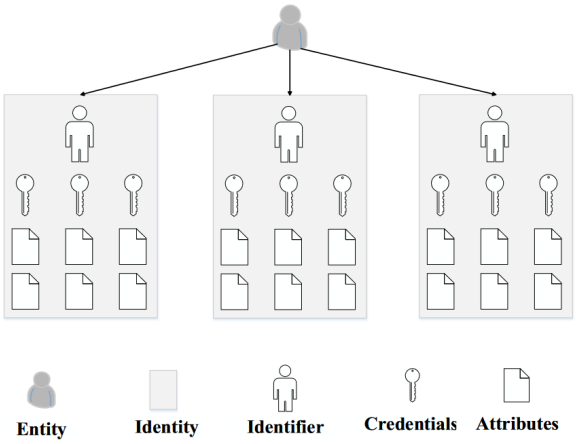
identidades voltada para IoT. Foi concebida uma identidade digital baseada em Blockchain e uma abordagem para o gerenciamento de identidades que garante uma identidade global e única para dispositivos. Além do registro e transferência de propriedade dos dispositivos, sua implementação oferece mecanismos para validação e rastreamento das identidades. Questões de escalabilidade não foram abordadas neste trabalho, mas constam como perspectivas futuras. Também não foram realizados experimentos para avaliar latência no processamento de transações.

3.3.3 *An Identity Management Framework for Internet of Things*

Em seu trabalho, (CHEN; LIU; CHAI, 2015) apresenta um framework para Gestão de Identidade voltada para IoT. Suas principais contribuições consistem em: um modelo informacional padrão para identidades no contexto de internet das coisas, uma arquitetura centrada no usuário e autenticação multi-canal. Segundo o autor, as principais características da IoT consistem em uma grande quantidade e variedade de dispositivos inteligentes, uma estrutura de rede distribuída e descentralizada, e uma ampla gama de aplicativos e cenários. Em um cenário ideal da IoT, quase tudo está conectado à internet, e existe extensa comunicação e interação entre os dispositivos inteligentes dos usuários e os serviços da Internet.

Devido à esta grande diversidade de dispositivos, ao amplo escopo de interações e outras características da IoT, considera-se que os modelos tradicionais de Gestão de Identidade para a Internet precisam ser estendidos e melhorados. Em seu trabalho, o conceito de identidade se estende a dispositivos, coisas e serviços. A Figura 8, apresenta o modelo de identidades proposto pelo autor. No modelo, cada entidade pode possuir múltiplas identidades, e cada identidade possui um identificador e um conjunto de credenciais e atributos.

Figura 8 – Modelo de Identidade.

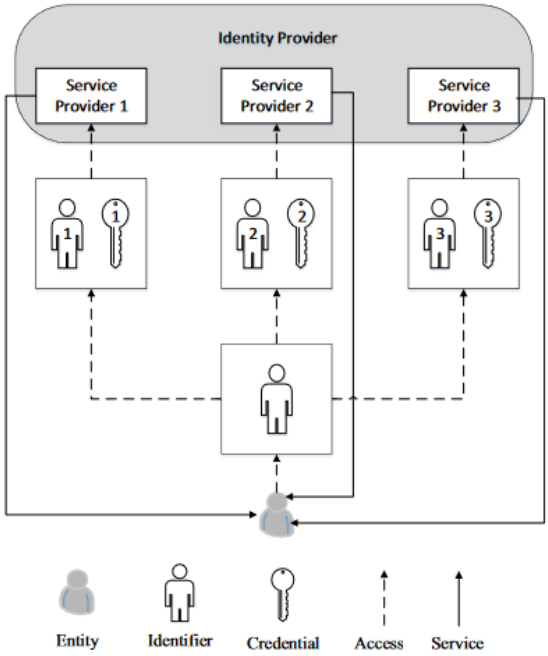


Fonte: (CHEN; LIU; CHAI, 2015).

O modelo informacional de identidades voltado para IoT, é composto por conjuntos

de informações essenciais. O primeiro é o conjunto de identificadores, composto por identificadores globais gerados pelo provedor de identidade global e identificadores locais gerados pelo provedor de identidade local. O segundo conjunto é de credenciais, que são comprovações de identidade, acesso ou crédito emitidas pelo provedor de identidade para uma entidade, podendo uma entidade possuir várias credenciais. Em seguida, tem-se o conjunto de atributos, contendo propriedades que descrevem a entidade em diferentes contextos. Por fim, o conjunto de informações de autorização registra as autorizações entre provedores de identidade e provedores de serviço, ou entre diferentes provedores de serviço. A Figura 9, apresenta a arquitetura geral da solução proposta pelo autor.

Figura 9 – Arquitetura proposta.



Fonte: (CHEN; LIU; CHAI, 2015).

Nesta arquitetura proposta, é necessário um provedor de identidade global. O provedor de identidade global é responsável por manter a identidade global, enquanto os provedores de serviços geram identidades locais de acordo com a identidade global e mantêm a consistência das informações com a identidade global. Cada identidade local pode ter sua própria credencial e método de autenticação. Por exemplo, um usuário pode desbloquear seu smartphone usando autenticação por impressão digital, enquanto acessa o sistema de controle de acesso de sua empresa por meio de autenticação por reconhecimento facial.

3.3.4 *Developing an IoT Identity Management System Using Blockchain*

Em (VENKATRAMAN; PARVIN, 2022), o autor propõe um sistema de gerenciamento de identidade baseado em blockchain para o ecossistema IoT de uma organização

para democratizar o controle de acesso a dispositivos IoT, privacidade de dados e confiança. Dentre os ativos de computação existentes no ecossistema estão presentes dispositivos IoT, componentes de software, usuários e operações de dados. Segundo o autor revisões da literatura apontam que a tecnologia *blockchain* vem sendo explorada para abordar problemas de segurança e privacidade existentes nos sistemas atuais de gestão de identidade. De acordo com o autor, a crescente integração da IoT na vida cotidiana destaca a necessidade crítica de soluções robustas de gerenciamento de identidade digital e privacidade de dados. Sua motivação baseia-se no fato de que os sistemas atuais de gerenciamento de identidade digital são insuficientes para lidar com os crescentes riscos de segurança e privacidade existentes na *internet*, e que as constantes falhas de segurança e vazamentos de dados evidenciam este fato. Frequentemente provedores de serviço atuam também como provedores de identidade gerando assim redundância dos dados e aumentando a exposição de usuários a riscos de segurança tais como coleta e uso não autorizado de dados pessoais.

Suas principais contribuições, (I) propor um novo modelo para gestão de identidades, baseado em blockchain, para IoT, que aborda privacidade de dados, e outros problemas de segurança associados a arquiteturas centralizadas; (II) demonstrar a aplicação de contratos inteligentes para habilitar transações auditáveis, preservadoras de privacidade e com políticas de controle de acesso; (III) desenvolver um estudo de caso como prova de conceito do modelo proposto. O estudo de caso no qual se baseia o trabalho, consiste em uma organização enfrentando problemas com o sistema de gerenciamento de identidade atualmente em uso. Há uma falta de soluções técnicas para apoiar o crescimento dos recursos de computação com vários dispositivos IoT conectados à infraestrutura de rede da organização. O sistema de gerenciamento de identidade atual não acompanha automaticamente as transações de uso ou atualização dos ativos da empresa em um ambiente altamente seguro e federado ou em um framework de confiança distribuído. Atualmente, a auditoria e o rastreamento dos registros de transações para cada recurso de computação ou ativo digital é feita de forma manual, o que torna frágil o processo de auditoria e responsabilização e facilita o uso não autorizado de informações. Dessa forma, foi projetado e desenvolvido um protótipo de prova de conceito utilizando uma plataforma de blockchain federada e distribuída com contratos inteligentes para oferecer suporte ao armazenamento altamente confiável de dados e à autenticação segura de recursos e operações de IoT dentro do cenário de caso de negócios.

Em seu modelo, todas as operações são feitas por meio de quatro contratos inteligentes que fazem a gestão das identidades de: recursos computacionais, recursos de software, usuários e *backup* de dados. Cada uma dessas categorias de recursos é composta por atributos e os contratos inteligentes implementam as lógicas de negócio do estudo de caso. A tecnologia blockchain oferece uma solução promissora para possibilitar o gerenciamento de identidades digitais de forma segura, com privacidade de dados e controle de acesso para dispositivos IoT.

3.3.5 *DAG Blockchain-based Lightweight Authentication and Authorization Scheme for IoT Devices*

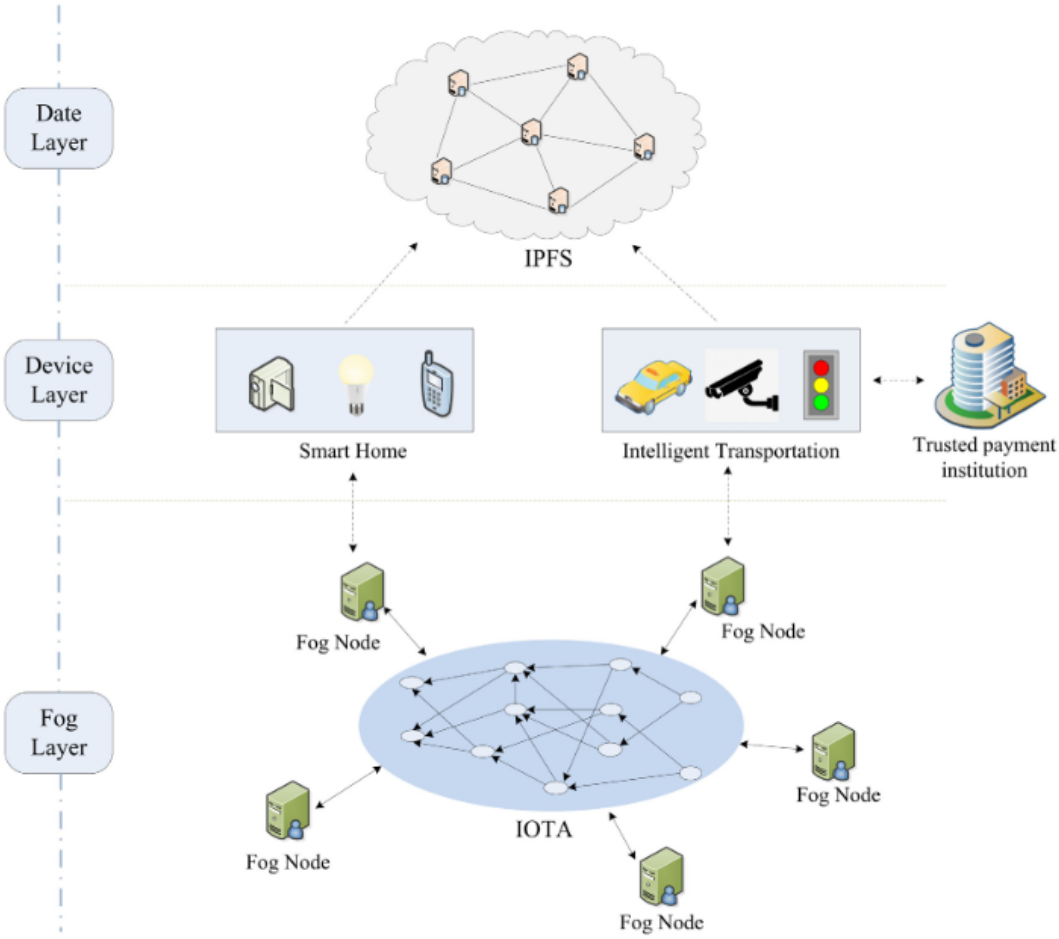
Em (WANG *et al.*, 2022) o autor propõe um mecanismo leve e escalável para gerenciar a identidade de dispositivos IoT e controlar o acesso de dados de IoT em larga escala com objetivo de garantir a confiabilidade da fonte dos dados e a segurança no compartilhamento de dados de IoT. Para isso, o autor explora a tecnologia de *ledger* distribuído `IOTA` para realizar as funções de registro, atualização, revogação e recuperação da identidade de dispositivos IoT. O autor considera que sistemas de gestão de identidade tradicionais baseados em infraestrutura de chaves públicas já oferecem serviços de segurança tais como autenticação de identidades, integridade de dados, confidencialidade e não repúdio, e que isto satisfaz requisitos de segurança para IoT. Porém existem limitações nestes sistemas tradicionais que são evidenciadas na medida que o número de dispositivos conectados cresce, dentre elas cita-se: pontos únicos de falha, dificuldade na gestão e instalação de certificados de dispositivos IoT, baixa eficiência na emissão de certificados e dificuldade de manter a lista de certificados raiz.

A arquitetura do sistema é apresentada na Figura 10, nela existem três camadas. A camada de dispositivos é composta por dispositivos IoT heterogêneos com recursos computacionais limitados em termos de processamento e armazenamento. Tais dispositivos coletam dados em tempo real para fornecer uma variedade de serviços. Em seu modelo apenas dispositivos IoT portadores de identidade podem participar de uma série de atividades de rede. A camada de dados usa a tecnologia *The InterPlanetary File System* (IPFS) para armazenar dados, o IPFS consiste em um conjunto modular de padrões e protocolos para organizar e mover dados utilizando redes *Peer-to-Peer* (p2p) (BENET, 2014). Os dados gerados pelo dispositivo IoT são criptografados e enviados para o IPFS. Os usuários podem obter dados criptografados diretamente do IPFS. Este sistema de armazenamento distribuído resolve o ponto único de falha causado por servidores de armazenamento de dados centralizados. A camada de névoa é uma rede composta por uma série de nós de névoa que servem como pontos de acesso para dispositivos IoT acessarem a rede. Cada nó de névoa gerencia um grupo de dispositivos IoT mais próximos a ele, o que assume grande parte do trabalho computacional dos dispositivos IoT. Isso reduz significativamente a carga desses dispositivos e sistemas leves, além de resolver o problema de latência na transmissão de dados na rede.

3.4 Comparação dos Trabalhos Relacionados

A Tabela 2 apresenta um quadro comparativo entre os trabalhos apresentados de acordo com critérios que tornam um sistema de gestão de identidades adequado para o contexto da CI. A escalabilidade é fundamental para garantir que o modelo possa lidar com

Figura 10 – Arquitetura do sistema proposto.



Fonte: (WANG *et al.*, 2022)

o grande número de dispositivos e atores presentes em uma CI. A disponibilidade é crucial para assegurar que o sistema possa mitigar ou eliminar possíveis pontos únicos de falha, garantindo assim a continuidade dos serviços. Mecanismos de governança transparentes e bem definidos são importantes tanto para a flexibilidade do modelo, permitindo a inclusão de novos *stakeholders* e entidades envolvidas na gestão das identidades, quanto para a segurança e confiança do modelo. A descentralização, por sua vez, garante que o modelo suporte a emissão descentralizada de identidades de dispositivos, sem depender de uma única entidade centralizadora. Por fim, a existência de uma implementação concreta do modelo ou a facilidade em utilizá-lo para desenvolver aplicações de IoT e cidades inteligentes é essencial para sua efetiva aplicação em cenários reais.

- `Escalabilidade`: Refere-se ao modelo abordar questões de escalabilidades para atender uma cidade, por exemplo: relação à quantidade de dispositivos/atores identificados/transações efetuadas.
- `Disponibilidade`: Refere-se ao modelo ser capaz de mitigar ou eliminar pontos únicos de falha.

- `Governança`: Diz respeito à flexibilidade do modelo para permitir a inclusão de novos *stakeholders* ou entidades que gerenciam as identidades.
- `Descentralização`: Refere-se ao modelo suportar a emissão descentralizada de identidades de dispositivos, não havendo apenas uma única entidade centralizadora no controle das identidades.
- `Implementação` (CI): Diz respeito à existência de implementação concreta do modelo, ou à facilidade em utilizar o modelo para desenvolver aplicações de IoT e CI.
- `Voltado para CI`: Diz respeito ao modelo ter sido especificado considerando as necessidades de cidades inteligentes.

Tabela 2 – Comparação de trabalhos relacionados

Trabalho	**Escal.**	**Dispon.**	**Gov.**	**Descen.**	**Impl.**	**CI**
(BOURAS *et al.*, 2021)	Sim	Sim	Sim	Sim	Sim	Não
(OMAR; BASIR, 2018)	Parcial	Sim	Sim	Semi	Parcial	Não
(CHEN; LIU; CHAI, 2015)	Sim	Sim	Não	Sim	Não	Não
(VENKATRAMAN; PARVIN, 2022)	Parcial	Sim	Sim	Não	Sim	Não
(WANG *et al.*, 2022)	Sim	Sim	Sim	Sim	Sim	Não

3.4.1 Discussão dos Trabalhos Relacionados

A escalabilidade de um modelo de gestão de identidades é fundamental quando se leva em conta a aplicação no contexto das CIs, onde existem uma serie de outros atores além dos dispositivos IoT. O modelo apresentado por (BOURAS *et al.*, 2021) utiliza a plataforma de *blockchain* `Hyperledger Fabric` e implementa contratos inteligentes para reger as operações de registro, autenticação e revogação de identidades. Para atender a um número maior de requisições de forma simultânea, e consequentemente aumentar a escalabilidade do modelo em termos de transações efetuadas o autor utiliza três *ledgers* distintos, um para cada operação da gestão de identidades. Em (OMAR; BASIR, 2018) foi proposto um modelo de gestão de identidades baseado *blockchain* que prevê um mecanismo para identificação única e global de dispositivos, um modelo de ciclo de vida de identidades, e os processos para registro, transferência de posse e rastreabilidade do ciclo de vida de um dispositivo. O autor não aborda diretamente questões de escalabilidade do modelo nem apresenta avaliações relativa a quantidade de operações suportadas. Apesar disso ele propõe um mecanismo de identificação única e global para dispositivos baseado em *hashs* de um conjunto mínimo de atributos que identificam unicamente o dispositivo. Dessa forma o autor atende parcialmente o quesito de escalabilidade quando considera o mecanismo para identificação global de uma quantidade grande de dispositivos. Em (CHEN; LIU; CHAI, 2015) foi proposto um modelo informacional padrão para identidades voltadas

para IoT, uma arquitetura de gestão de identidades centrada no usuário e mecanismos de autenticação entre os participantes de ambientes IoT. A arquitetura de Gerenciamento de Identidade centrada no usuário possibilita que o usuário tenha acesso a diferentes serviços de IoT por meio de diferentes métodos de autenticação sem precisar manter múltiplas identidades. Em sua implementação o autor utiliza um provedor de identidades global aliado a diversos provedores de identidade locais que eventualmente sincronizam com o provedor global. Este mecanismo de provedores locais permite com que o autor suporte um maior número de dispositivos IoT identificados por seu modelo. Em (VENKATRAMAN; PARVIN, 2022) foi apresentado um modelo de gestão de identidades que atende um caso de uso específico em uma empresa privada. O modelo lida de forma satisfatória com os diversos dispositivos existentes no contexto de aplicação apresentado. Apesar disso, o autor destaca que a escalabilidade do modelo proposto ainda precisa ser avaliada para operações de larga escala, e que atualmente o modelo é limitado, em termos de quantidade de transações efetuadas, pela taxa de transferência da rede *blockchain* utilizada. Em (WANG *et al.*, 2022) o autor propõe um mecanismo leve e escalável para gerenciar a identidade de dispositivos IoT e controlar o acesso de dados de IoT em larga escala com objetivo de garantir a confiabilidade da fonte dos dados e a segurança no compartilhamento de dados de IoT. Seu modelo de gestão de identidades é escalável e adequado para lidar com cenários puramente de IoT, que possuem grande quantidade de dispositivos IoT heterogêneos. Apesar disso, não estão previstos outros atores existentes em CI.

Todos os trabalhos relacionados atendem ao critério da disponibilidade, que refere-se a capacidade de eliminar pontos únicos de falha. O uso da tecnologia *blockchain* para concepção de sistemas de gestão de identidades é capaz de prover esta característica, assim como outras características tais como transparência dos registros e operações efetuadas. A governança também é uma característica que pode ser herdada em muitos casos através da utilização de *blockchain*. Em sua maioria os trabalhos também oferecem meios transparentes para a gestão das identidades que são feitas por meio de contratos inteligentes, onde mantém-se de forma imutável os registros das operações. Considerou-se que em (CHEN; LIU; CHAI, 2015) este critério não foi satisfeito por conta do modelo não possuir implementação concreta e se tratar apenas de uma proposta de modelo informacional para gestão de identidade. Em (VENKATRAMAN; PARVIN, 2022), apesar de ser uma solução para um cenário específico de uma empresa, considera-se que o critério foi atendido uma vez que o modelo foi capaz de mitigar os problemas relacionados ao acesso à dispositivos e à falta de auditoria.

Em sua maioria, os trabalhos relacionados também atendem ao critério da descentralização uma vez que utilizam a tecnologia *blockchain*. A tecnologia *blockchain* é capaz de descentralizar a gestão das identidades, eliminando assim os riscos de existir apenas uma organização no controle de todas as informações e também os eventuais intermediários. Em (OMAR; BASIR, 2018), o próprio autor classifica seu modelo de

gestão de identidades como semi-descentralizado. Apesar disso, não existem no texto outras referências ou justificativas para esta classificação. Por isso este trabalho foi classificado como semi-descentralizado conforme apresentado pelo autor. Em (VENKATRAMAN; PARVIN, 2022) considerou-se que o autor não atende aos critérios da descentralização uma vez que sua solução é dedicada ao ambiente de uma empresa e portanto todo o controle de emissão das identidades está sob apenas uma organização.

Em sua maioria os trabalhos também apresentam implementação concreta do modelo, atendendo assim ao critério estabelecido. Como exceção, temos (CHEN; LIU; CHAI, 2015), que apresenta apenas um modelo informacional bem definido para gestão das identidades porém não o implementa. Em (OMAR; BASIR, 2018) o autor apresenta seu modelo e implementa os contratos inteligentes que regem a gestão de identidade, porém não foram apresentados casos de uso ou aplicações reais do modelo para desenvolver aplicações de IoT e CI.

A comparação dos trabalhos relacionados com a solução proposta nesta dissertação será apresentada ao final do próximo capítulo.

4 Solução Proposta

Neste capítulo, será apresentada a solução proposta, que consiste em um modelo de gestão de identidades baseado em *blockchain* e voltado para CI. Além disso, será discutida a implementação dos componentes de *software* que compõem a solução e também sua integração com a plataforma *InterSCity*. Ao fim, será feita uma comparação desta solução em relação aos critérios abordados no capítulo de trabalhos relacionados.

4.1 Modelo de Gestão de Identidades

Um modelo de gestão de identidades voltado para cidades inteligentes deve ser capaz de atender as necessidades deste ambiente. Para discutir estas necessidades retomaremos o cenário de um ônibus inteligente que possui dois dispositivos IoT instalados, um para coletar e transmitir as coordenadas geográficas do ônibus, e outro para transmitir imagens em tempo real do interior do veículo a partir de uma câmera de segurança. A partir dos dados coletados por estes dispositivos seriam implementados serviços para processamento dos dados e extração de informações que seriam utilizadas por gestores para melhor gerir os recursos da cidade. Poderiam ainda ser desenvolvidas aplicações para a cidade, por exemplo: uma aplicação de mobilidade urbana que informa as rotas e calcula o tempo de chegada nos ônibus nas estações para o conforto dos cidadãos. Naturalmente neste cenário os dispositivos IoT, serviços e aplicações fariam parte de diferentes entidades administrativas do poder público que possuem atribuições diferentes e objetivos diferentes. Por exemplo, enquanto um dispositivo que transmite as coordenadas de um ônibus inteligente é mantido pela secretaria de transporte, as câmeras de segurança são mantidas pela secretaria de segurança pública.

Neste ecossistema complexo de uma CI um modelo de gestão de identidades ideal deve ser capaz de identificar unicamente as entidades administrativas, assim como dispositivos IoT, serviços e aplicações que podem estar associados as entidades administrativas. Neste cenário a descentralização do modelo é fundamental, uma vez que a centralização poderia causar pontos únicos de falha capazes de comprometer os serviços de segurança de toda a cidade. Como os serviços da cidade envolvem dados sensíveis e são mantidos com dinheiro público é imperativo que um modelo de gestão de identidades aplicado a este cenário seja completamente transparente e auditável. Resguardar os recursos da cidade por meio da identificação, autorização e responsabilização dos atores que realizam ações dentro do ecossistema da cidade é fundamental para garantir um ambiente seguro.

A solução proposta nesta dissertação consiste em um modelo de gestão descentralizado de identidades voltado para CI. No modelo, considera-se obrigatório a identificação

de todos os atores que interagem no complexo ecossistema de uma CI com intuito de permitir o desenvolvimento de serviços de segurança de forma descentralizada, democrática, transparente e auditável. Também considera-se que a gestão e controle da cidade como um todo é feita de forma colaborativa por Entidades Administrativas do poder público que, apesar de terem o mesmo objetivo final de contribuir com a cidade, possuem atribuições e responsabilidades independentes. Também é necessário oferecer mecanismos transparentes para gestão das identidades ao longo do ciclo de vida dos atores identificados.

No modelo proposto as Entidades Administrativas atuam de forma independente e atuam como emissoras de identidades digitais para identificar quaisquer outros atores existentes, sejam eles dispositivos IoT, sensores, atuadores, componentes de *software*, funcionários públicos, etc. A seguir são apresentados os atores que foram considerados no modelo proposto.

- **Entidades Administrativas do Poder Público**: estas entidades incluem órgãos governamentais e administrativos responsáveis pela gestão e operação da cidade, tais como prefeituras, sub-prefeituras, secretarias e etc. Elas precisam de acesso seguro e controlado às informações e aos sistemas da cidade para tomar decisões e gerenciar os recursos da cidade de forma eficientemente.
- **Dispositivos IoT:** estes dispositivos estão distribuídos por toda a cidade, coletando e transmitindo dados em tempo real. Eles podem incluir sensores de trânsito, medidores de energia, câmeras de segurança, viaturas, entre outros. A identificação e autenticação segura desses dispositivos são cruciais para garantir a integridade e a confiabilidade dos dados.
- **Componentes de Software**: softwares que processam e analisam os dados coletados pelos dispositivos IoT. Estes podem incluir sistemas de gerenciamento de tráfego, plataformas de análise de dados urbanos, aplicativos de serviços públicos, dentre outros. A autenticação desses componentes garante que apenas softwares autorizados possam acessar e manipular os dados sensíveis da cidade.
- **Outros Atores:** este grupo pode incluir empresas privadas, fornecedores de serviços, funcionários públicos e dentre outros *stakeholders* que interagem com a infraestrutura da cidade inteligente. A gestão de identidades para esses atores é fundamental para assegurar que apenas indivíduos e organizações autorizadas possam acessar os sistemas e dados relevantes.

Para implementação do modelo, utilizou-se uma *blockchain* permissionada na qual foram exploradas suas características como descentralização da informação, disponibilidade, privacidade, integridade, imutabilidade e auditabilidade para criar um repositório confiável de identidades digitais. As identidades dos atores são gerenciadas por Entidades

Administrativas através de operações que foram implementadas através de contratos inteligentes. A adoção de uma blockchain privada para implementação da solução oferece uma série de vantagens específicas para o contexto de IoT e CI. Em uma blockchain privada, o controle de acesso é restrito a participantes autorizados, proporcionando maior segurança e privacidade dos dados sensíveis, como informações pessoais dos cidadãos e credenciais dos dispositivos conectados. Esse modelo é ideal para cidades inteligentes, onde a proteção dos dados é essencial devido à grande quantidade de informações críticas que são geradas e compartilhadas continuamente. Além disso, uma blockchain privada permite um maior controle sobre as regras de governança, possibilitando que as autoridades locais ou as organizações responsáveis definam as políticas de validação e consenso. Outro fator importante é a capacidade de conformidade com regulamentações locais e internacionais sobre privacidade e proteção de dados. A blockchain privada oferece flexibilidade para implementar contratos intelige que garantam a conformidade com leis como a Lei Geral de Proteção de Dados no Brasil ou o Regulamento Geral de Proteção de Dados na Europa, enquanto ainda se beneficia da imutabilidade e auditabilidade fornecidas pela tecnologia blockchain.

4.2 Contratos Inteligentes: Registro, Autenticação e Revogação de Identidades

Para concepção do modelo de gestão de identidades baseado em *blockchain* foram implementados três contratos inteligentes que concentram todas as operações existentes no modelo proposto, sendo um contrato para as operações relacionadas a emissão de identidades, um para as operações de revogação de identidades e o último para o registro das autenticações efetuadas. O contrato de emissão de identidades permite com que a Entidade Administrativa possa registrar sua própria identidade em sua fase de inicialização e posteriormente emitir identidades para quaisquer outros atores que ficam registradas na *blockchain*. O contrato de revogação de identidades permite com que a Entidade Administrativa registre na *blockchain* aquelas identidades que foram revogadas e a partir daquele momento deixam de ser válidas. Este é caso por exemplo de um dispositivo IoT que chega ao fim de sua vida útil e precisa ter sua identidade revogada. O contrato de autenticação pode ser utilizado pelos atores para registrar na *blockchain* que uma autenticação ocorreu em algum determinado contexto de aplicação. Por exemplo, este é o caso em que um serviço precisa autenticar um dispositivo IoT antes de receber os dados transmitidos pelo dispositivo. Após o serviço autenticar o dispositivo IoT o serviço pode executar o contrato de autenticação para registrar na *blockchain* que essa operação foi feita. O histórico das transações enviadas a *blockchain* por meio dos contratos inteligentes é imutável, de forma a oferecer rastreabilidade das operações executadas. A implementação de contratos inteligentes também torna a lógica do modelo de gestão de identidades

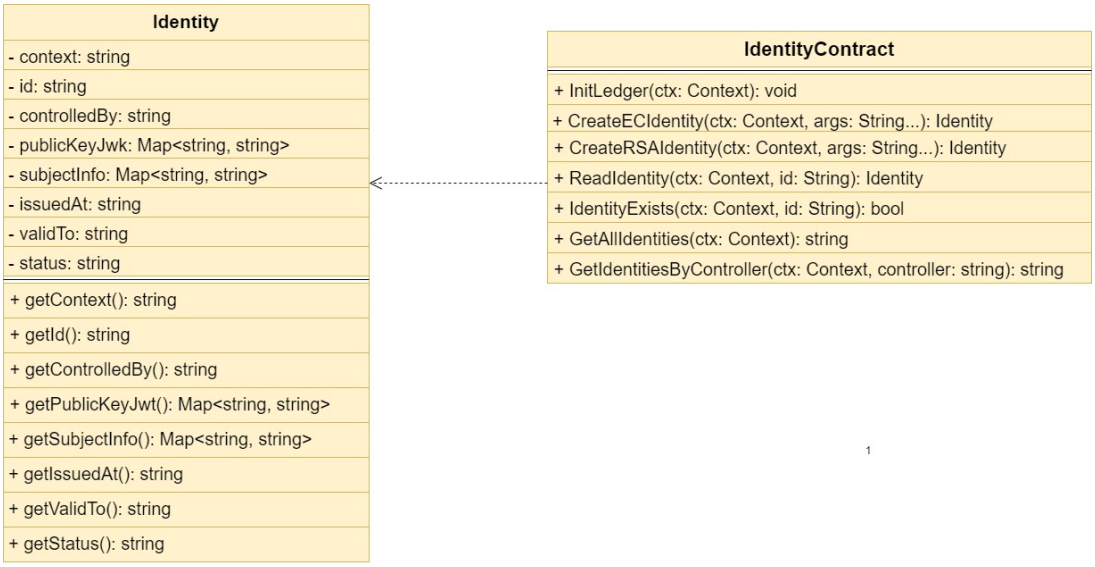
transparente e democrática para as Entidades Administrativas que fazem parte do modelo. O código implementado é público para os participantes e ele não pode sofrer alterações sem que as Entidades Administrativas participantes aprovem as alterações. Ao aplicar estes contratos no cenário descrito, podemos ter múltiplas Entidades Administrativas coexistindo de forma independente e emitindo as identidades de forma descentralizada. Não existe uma entidade em total controle do modelo, todas as Entidades Administrativas tem igual capacidade de emissão e revogação de identidades e os participantes podem registrar as autenticações realizadas.

A Figura 11 apresenta o diagrama de classes do contrato inteligente que rege o registro de identidades na *blockchain*. A classe `Identity` apresenta o modelo de dados que compões as identidades, enquanto a classe `IdentityContract` implementa os métodos do contrato inteligente. O modelo de identidades proposto é composto principalmente por um identificador único (**id**), por um controlador (**controlledBy**) ou em outras palavras a Entidade Administrativa emissora daquela identidade, por uma chave pública (**publicKeyJwt**), e por uma lista de atributos dinamicamente atribuídos no momento do registro (**subjectInfo**), que servem para identificar o sujeito daquela identidade (e.g., nome, fabricante, numero de série, etc). Os campos (**issuedAt**), (**validTo**) e (**status**) servem respectivamente para registrar a data de emissão, validade e estado atual da identidade. O processo de autenticação/validação de identidades é inteiramente realizado por meio de assinaturas digitais que utilizam o par de chaves criptográficas do portador da identidade. Como apenas a componente pública da chave é salva em *blockchain*, a componente privada deve ser armazenada em segurança pelo portador da identidade e mantida em segredo. Os métodos **CreateECIdentity** e **CreateRSAIdentity** são utilizados para emitir as novas identidades, os métodos **ReadIdentity** e **IdentityExists** são utilizados respectivamente para consultar identidades pelo identificador e para verificar a existência da identidade pelo identificador, por fim os métodos **GetAllIdentities** e **GetIdentitiesByController** recuperam respectivamente todas a identidades registradas e todas as identidades de um dado controlador.

Para geração das chaves criptográficas, adotou-se a criptografia de curva elíptica, ou *Elliptic-curve cryptography* (ECC) (P-256, P-384, P-521), pois este padrão garante o mesmo nível de segurança que as do tipo Rivest-Shamir-Adleman (RSA), porém utilizando tamanhos de chave menores (MEKTOUBI *et al.*, 2016). Esta escolha foi feita devido à típica restrição de recursos em dispositivos IoT. O armazenamento das chaves é feito segundo o formato *JSON Web Key* (JWK) (JONES, 2015). No modelo proposto, pressupõe-se que apenas dispositivos IoT capazes de realizar requisições *HTTP* [1] e gerar assinaturas digitais conseguem utilizar as identidades propostas. Alternativamente, pode-se empregar o modelo utilizando *gateways* para gerenciar os dispositivos e realizar tais operações em

[1] https://developer.mozilla.org/pt-BR/docs/Web/HTTP

Figura 11 – Diagrama de classe do modelo de identidade e do seu contrato inteligente.



Fonte: autoria própria.

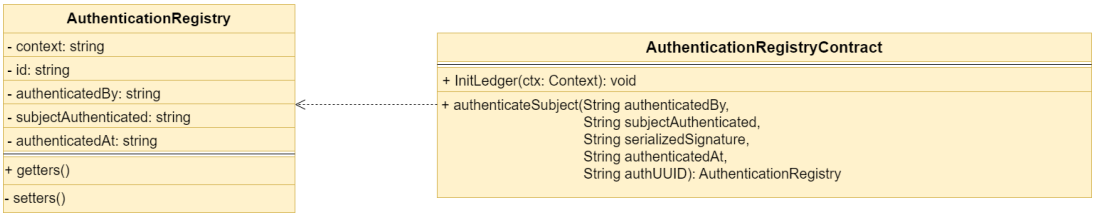
função deles.

O modelo estabelece uma hierarquia onde as Entidades Administrativas registram suas próprias identidades e, em seguida, podem gerar identidades para dispositivos IoT e outros atores. Adotaremos o termo identidade Raiz para se referir as identidades das Entidades Administrativas, que têm o poder de emitir novas identidades do tipo Folha. O termo identidade Folha será utilizado para se referir às identidades dos demais atores. Cada identidade folha está necessariamente associada a apenas uma identidade Raiz. Dessa forma, cada identidade traz consigo o identificador de seu controlador, o que torna as identidades rastreáveis e verificáveis a todo momento. Esta estrutura hierárquica assegura que todas as identidades sejam criadas e gerenciadas de forma controlada, promovendo uma gestão de identidades mais segura, transparente e eficiente em uma cidade inteligente. Como as componentes públicas das identidades são armazenadas na *blockchain*, dois atores quaisquer que queiram se comunicar podem utilizar as chaves criptográficas para garantir a procedência dos dados e garantir que de fato estão se comunicando com um com o outro. Por exemplo, ao transmitir uma mensagem sensível um ator pode criptografar a mensagem com sua chave privada e em seguida criptografar novamente com a chave pública do receptor. Dessa forma o receptor pode receber mensagens de forma segura sendo garantido que a mensagem de fato era para ele e que foi de fato enviada pelo transmissor. Por meio desse modelo, torna-se conveniente desenvolver aplicações seguras no contexto de uma cidade inteligente.

Também foram implementados outros dois contratos inteligentes, um para registrar as revogações de identidade, e outro para gerenciar as autenticações que são efetuadas no contexto das aplicações usuárias do nosso modelo. A revogação é uma operação fundamental para concluir o ciclo de vida de uma identidade, enquanto o registro das operações de

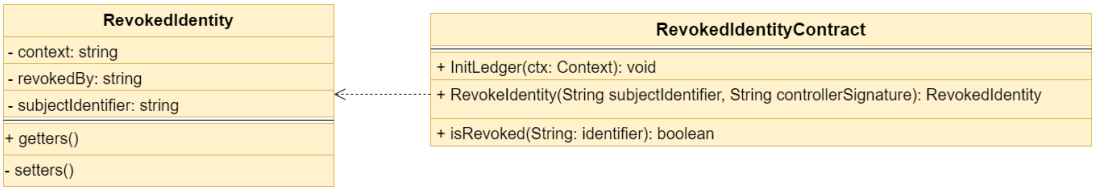
autenticação tem a finalidade de auditoria em relação as autenticações feitas. As Figuras 12 e 13 apresentam o diagrama de classe dos contratos de revogação de identidades e registro de autenticações e suas estruturas de dados. De forma similar ao contrato de identidades, a classe `AuthenticationRegistry` apresenta o modelo de dados que compõe o registro de autenticação que é formado por um identificador único (**id**), pelo identificador de quem realizou a autenticação (**autheticatedBy**), pelo identificador de quem foi autenticado (**subjectAuthenticated**) e pela data a autenticação (**autheticatedAt**). A data de autenticação é definida pelo próprio contrato inteligente como forma de evitar imprecisões relacionadas à dessincronização de relógios. A classe `AuthenticationRegistryContract` implementa os métodos do contrato inteligente, sendo o método `authenticateSubject` responsável por inserir o registro de autenticação na *blockchain*. Como parâmetros para autenticação é necessário que o autenticador prove sua identidade por meio de uma assinatura digital que é validada pelo contrato inteligente antes do registro ser inserido. Essa regra de negócio garante que é de fato a Entidade Administrativa correta é quem esta inserindo os registros. A classe `RevokedIdentity` apresenta o modelo de dados que compõe um registro de revogação de identidade no qual estão presentes o identificador da Entidade Administrativa que revoga a identidade (**revokedBy**) e o identificador da identidade revogada (**subjectIdentifier**). A classe `RevokedIdentityContract` implementa os métodos do contrato inteligente, nela está presente o método `RevokeIdentity` que recebe como parâmetro o identificador da identidade a ser revogada e uma assinatura digital que supostamente é do controlador daquela identidade. O próprio contrato inteligente foi implementado para obter o controlador da identidade alvo diretamente da *blockchain* e validar contra a assinatura apresentada. Caso a assinatura esteja correta (i.e., seja do controlador da identidade) a revogação daquela identidade é registrada na *blockchain*.

Figura 12 – Diagrama de classe do registro de autenticações e seu contrato inteligente.



Fonte: autoria própria.

Figura 13 – Diagrama de classe do registro de revogações e seu contrato inteligente.



Fonte: autoria própria.

Por meio desses três contratos inteligentes, foram implementadas as seguintes regras de negócio que regem o modelo de gestão de identidades:

- Toda Entidade Administrativa possui uma identidade do tipo raiz, que pode ser utilizada para emissão de novas identidades folha;
- Para incluir uma nova identidade, a Entidade Administrativa precisa informar qual o endereço de sua identidade (i.e., seu identificador) e uma assinatura digital como forma de autenticação. Após a validação dessa assinatura pelo contrato inteligente, a nova identidade pode ser inserida na rede;
- As revogações de identidade são feitas pelas Entidades Administrativas, mediante apresentação de sua assinatura digital, de forma que apenas o controlador da identidade tem autorização para revoga-la. Essa verificação é feita por meio do contrato inteligente.
- Qualquer participante da rede pode autenticar outro participante e essa operação deve ser registrada na rede. Para isso, um participante deve possuir uma assinatura digital da contraparte que deseja autenticar. O contrato inteligente valida a assinatura apresentada e caso seja válida fica registrado na rede que um participante concluiu a operação de autenticação em relação a outro participante.

4.3 Relacionamentos Entre os Atores

As Entidades Administrativas desempenham um papel central em nosso modelo gerenciando as identidades dos demais atores presentes em uma CI. Os dispositivos IoT, aplicações e quaisquer outros atores possuem uma relação de dependência com a Entidade Administrativa, uma vez que sua existência no modelo proposto está condicionada a uma dessas entidades. Dessa forma, podemos descrever os relacionamentos entre as entidades e demais atores em função de ações que podem ser desempenhadas no contexto de uma CI:

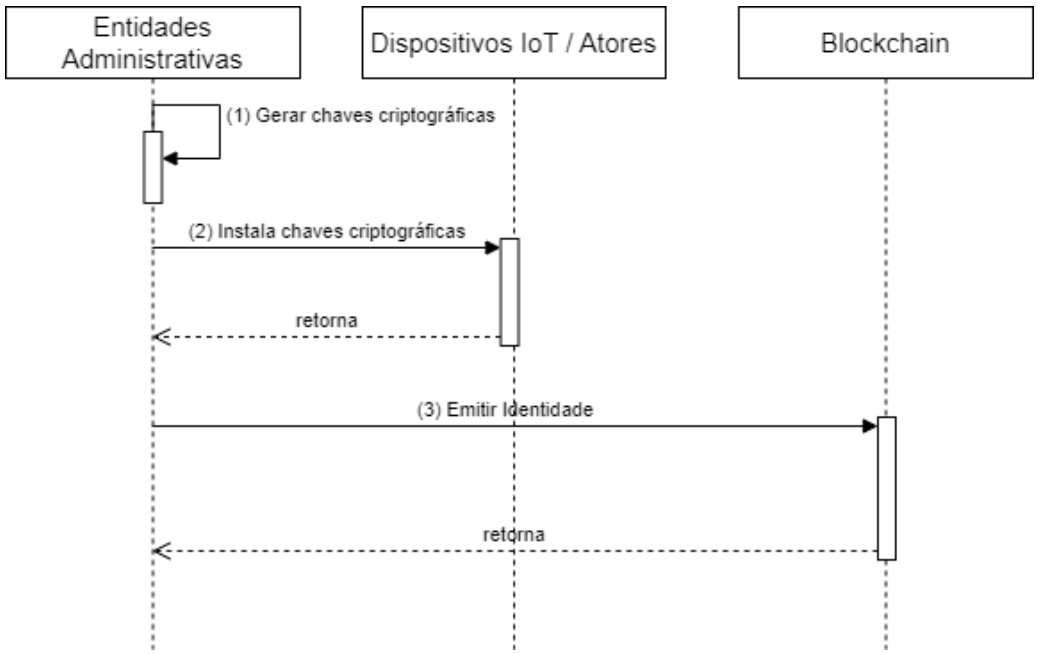
1. Instalação de dispositivos de IoT;
2. *Deployment* de aplicações de CI;
3. Coleta e envio de dados por dispositivos de IoT;
4. Manutenção e remoção de dispositivos de IoT;

4.3.1 Instalação de Dispositivos de IoT

No modelo proposto, cabe as Entidades Administrativa instalarem os dispositivos IoT na cidade. Este processo é ilustrado na Figura 14 que apresenta um diagrama de

sequência abordando o processo de (1) geração das chaves criptográficas, (2) instalação das chaves no dispositivo e (3) registro da identidade do dispositivo na *blockchain*. Conforme já comentado, toda identidade possui uma Entidade Administrativa como sua controladora, a única exceção é a própria identidade da Entidade Administrativa que aponta para si mesma como sua controladora. No modelo proposto as chaves criptográficas devem ser geradas e instaladas no dispositivo de forma *offline* para diminuir o risco de vazamento das chaves durante transmissão. Apenas a componente pública é registrada na *blockchain* e associada a identidade do dispositivo.

Figura 14 – Diagrama de sequência da instalação de novo dispositivo.



Fonte: autoria própria.

4.3.2 *Deployment* de Aplicações de CI

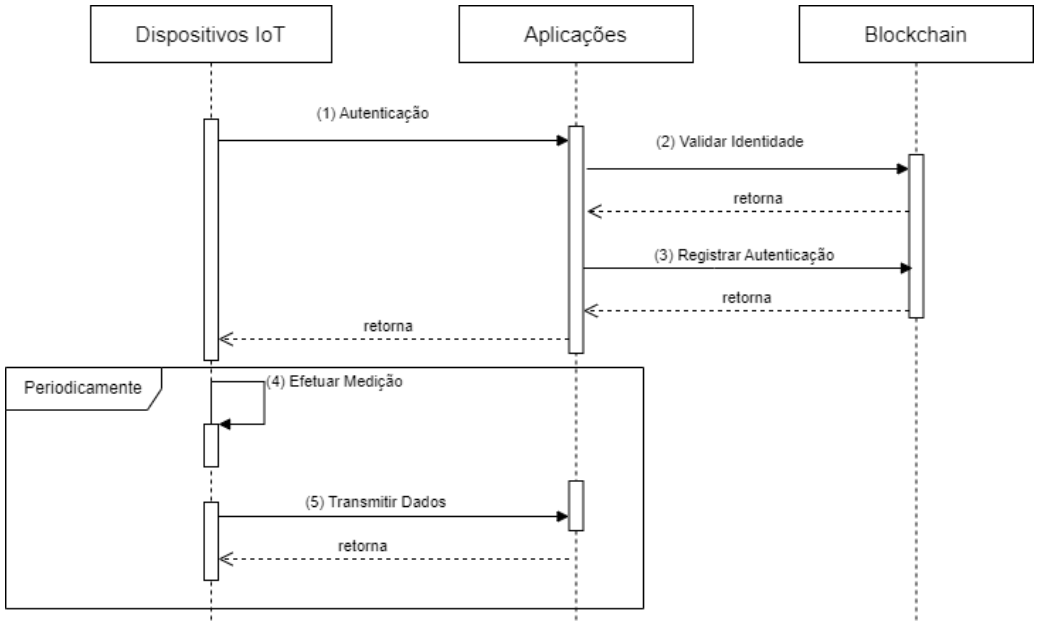
Serviços e aplicações de CI estão previstas no modelo proposto e também são atores passíveis de identificação. Ao atribuir identidades para componentes de *software* torna-se possível desenvolver mecanismos de segurança capazes de levar em conta os dispositivos IoT e demais atores. Podemos tomar como exemplo uma aplicação de mobilidade urbana que recebe dados transmitidos por um dispositivo IoT portador de uma identidade. Neste caso torna-se possível desenvolver mecanismos para autenticação mutua entre aplicação e dispositivo usando as identidades do modelo proposto.

4.3.3 Coleta e Envio de Dados por Dispositivos de IoT

Dispositivos e *gateways* IoT existentes em uma cidade inteligente são responsáveis pela coleta e transmissão de dados que são utilizados pela gestão da cidade durante o processo de tomada de decisões estratégicas. No modelo proposto ao identificar os

dispositivos podemos implementar os mecanismos necessários para garantir a procedência dos dados coletados e assim tomar decisões em cima de dados corretos, transmitidos por dispositivos autenticados. A Figura 15 ilustra o processo no qual um dispositivo IoT (1) se autentica com uma aplicação e então a aplicação (2) valida sua identidade diretamente na *blockchain* e após validação (3) registra na *blockchain* que a operação de autenticação ocorreu, após isso o dispositivo pode (4) efetuar suas medições e (5) transmitir os dados coletados.

Figura 15 – Diagrama de sequência da coleta e envio de dados por dispositivos de IoT.



Fonte: autoria própria.

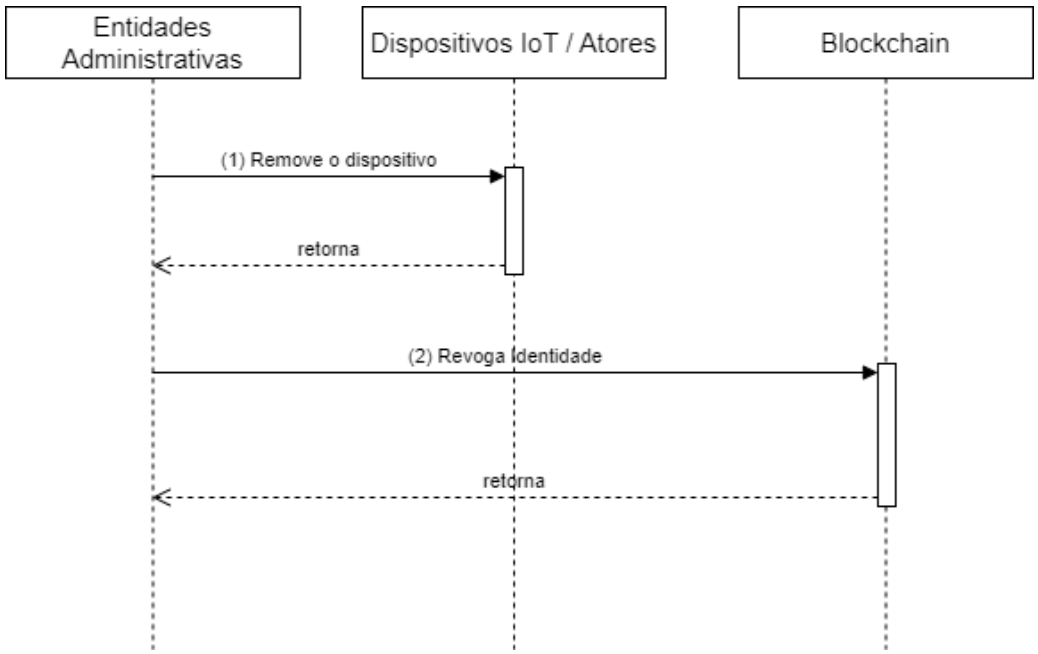
4.3.4 Manutenção e Remoção de Dispositivos de IoT

Todo dispositivo IoT possui um ciclo de vida definido, após ser instalado eventualmente ele pode ser avariado, ou chegar a fim de sua vida útil pode diversos motivos. A revogação das identidades impede que a elas sejam usadas em autenticações após a revogação. A Figura 16 aborda o processo na qual a Entidade Administrativa (1) remove fisicamente o dispositivo IoT e então (2) revoga a identidade na *blockchain*, a partir deste momento a identidade passa a fazer parte da lista de revogações que pode ser consultada a qualquer momento pelos demais atores.

4.4 Implementação do Modelo de Gestão de Identidades

Após a especificação o modelo foi implementado através de componentes de software e dos contratos inteligentes de autenticação, revogação e registro de autenticações. Além disso, o modelo foi integrado a plataforma *InterSCity* para o desenvolvimento de serviços de

Figura 16 – Diagrama de sequência da remoção de dispositivos de IoT.



Fonte: autoria própria.

segurança, inexistentes até então, voltados para a coleta, distribuição dos dados de IoT para a plataforma. A escolha do *Hyperledger Fabric* para a implementação da solução proposta deve-se principalmente à sua flexibilidade e robustez em suportar contratos inteligentes. O *Hyperledger Fabric* oferece uma arquitetura modular que permite a customização de diversos componentes, como o consenso e a gestão de identidades, o que facilita a adaptação do sistema às necessidades específicas do gerenciamento de identidades no contexto de blockchain. Além disso, a sua capacidade de suportar contratos inteligentes programados em linguagens como *Java*, *Go* e *Node.js*, garante um ambiente propício para a criação de lógicas de negócio complexas e personalizadas. A capacidade de criar canais privados para transações confidenciais também foram fatores determinantes para a escolha dessa tecnologia, considerando que a segurança e a confidencialidade são aspectos críticos no gerenciamento de identidades em ambientes distribuídos tais como ambientes de IoT e CI.

O InterSCity é um projeto colaborativo de pesquisa que abrange nove instituições nacionais e parceiros internacionais. A plataforma *InterSCity* (ESPOSTE *et al.*, 2017) foi criada para dar suporte ao desenvolvimento de projetos e aplicações de IoT, Big Data e Computação em Nuvem. A plataforma modela a CI como sendo composta por recursos da cidade (e.g., um ônibus inteligente, semáforo inteligente, viaturas, ou qualquer outro recurso físico). Cada recurso pode conter diversas capacidades que representam um modelo de dados que o recurso pode disponibilizar. Por exemplo, um ônibus inteligente é um exemplo de recurso da cidade, que pode possuir várias capacidades, tais como: temperatura dentro do ônibus, intensidade de ruído no interior, coordenada geográficas, etc. Tais dados são tipicamente coletados através dispositivos IoT, e são publicados na plataforma para

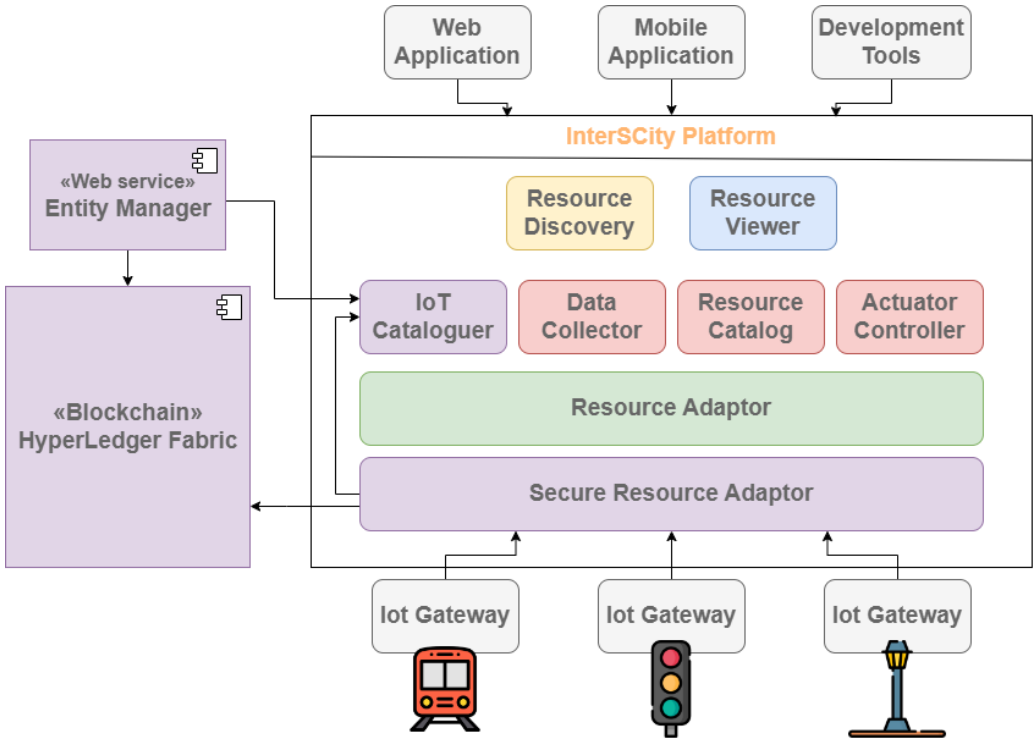
posterior consulta por parte de aplicações. Todos os dados inseridos na plataforma estão associados a um recurso e a uma capacidade. Uma vez que algum dispositivo efetue essas leituras de sensoriamento e registre os dados na plataforma, as aplicações de cidades inteligentes podem consumir os dados através dos microsserviços do *InterSCity* filtrando os dados em termos de recursos e capacidades.

Desenvolveu-se novos microsserviços que se integram ao *InterSCity* e oferecem mecanismos para autenticar os dispositivos IoT que se conectam na plataforma, assim como garantir controle sobre quais tipos de dados cada dispositivo tem direito de publicar na plataforma. A Figura 17 ilustra a arquitetura da plataforma *InterSCity* com a adição dos novos componentes de software que utilizam nosso modelo proposto para prover autenticação e controle de admissibilidade sobre os dispositivos de IoT. Os componentes de *software* desenvolvidos utilizam a *blockchain* para gerir as identidades propostas no modelo, e foram integrados à plataforma *InterSCity*. Tais componentes são destacados na imagem na cor roxa, ou púrpura, e são denominados: `Entity Manager`, `IoT Cataloguer`, `Secure Resource Adaptor` e a *blockchain*.

A seguir serão apresentados os microsserviços já existentes na plataforma *InterSCity* e posteriormente serão apresentados os novos componentes desenvolvidos que fazem uso do modelo proposto. O componente `Resource Adaptor` é responsável por receber os dados de sensoriamento provenientes de dispositivos ou *gateways* IoT, e persisti-los nas bases de dados da plataforma. O componente `Resource Catalog` é o responsável pelo registro de recursos da cidade e de suas respectivas capacidades. O componente `Data Collector` é utilizado por aplicações para consumo dos dados inseridos por dispositivos. Os demais componentes lidam com visualização de dados e envio de comandos de atuação. Através desses componentes, a plataforma facilita o desenvolvimento de aplicações de CI, de forma que múltiplos dispositivos podem ser implantados na cidade para coleta de dados, e aplicações podem consumir estes dados. Por exemplo, uma aplicação de mobilidade urbana pode consultar a plataforma para obter o valor da temperatura, localização ou qualquer outra capacidade daquele recurso específico (*i.e.*, ônibus inteligente).

À plataforma InterSCity não contava com mecanismos de autenticação e controle de acesso, de forma que uma instância do InterSCity não conseguia diferenciar produtores de dados ou impedir que algum dispositivo se passe por outro. Utilizando o modelo proposto para gerenciamento de identidades baseado em *blockchain*, desenvolveu-se uma infraestrutura de segurança para garantir mecanismos de autenticação e controle de acesso na escrita de dados. Para isto, desenvolveu-se três componentes de *software* denominados `Entity Manager`, `Secure Resource Adaptor` e `IoT Cataloguer`.

Figura 17 – Arquitetura geral da plataforma InterSCity, incluindo os novos componentes desenvolvidos.



Adaptado de: (ESPOSTE *et al.*, 2017).

4.4.1 Entity Manager

Para implementar o modelo proposto, que utiliza a tecnologia de *blockchain* para gestão descentralizada de identidades, foi desenvolvido um componente de *software* chamado `Entity Manager`. Este componente representa as Entidades Administrativas do modelo, sendo capaz de enviar transações à *blockchain* para executar os contratos inteligentes responsáveis pela emissão e revogação de identidades dos demais atores (i.e., dispositivos IoT, componentes de *software*, etc).

Este componente foi desenvolvido com o objetivo de abstrair as complexidades existentes na rede *blockchain* e na execução de contratos inteligentes. Portanto, seu principal objetivo é facilitar a emissão, recuperação e revogação de identidades. Tais funcionalidades oferecidas por este componente são disponibilizadas através de uma interface *API REST* [2]. Todas as identidades emitidas por uma Entidade Administrativa, através do componente de *software* `Entity Manager`, apontam para o emissor da identidade. Dessa forma, todas as identidades registradas na rede *blockchain* podem ser verificadas e rastreadas para determinar a Entidade Administrativa emissora da identidade.

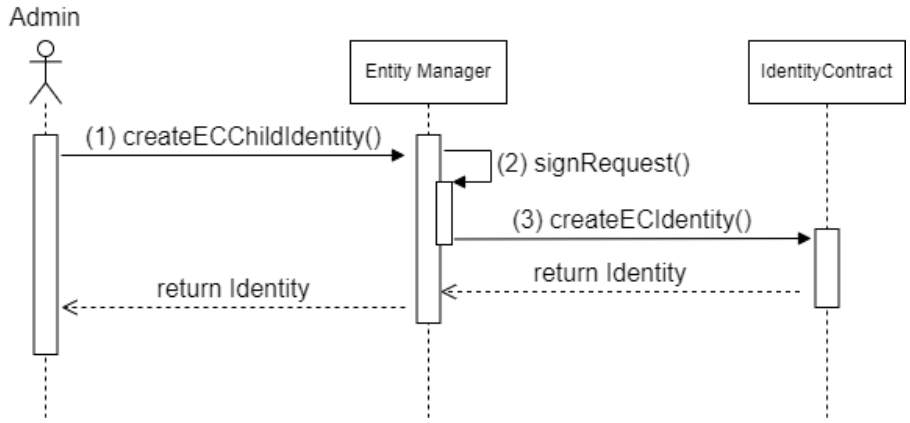
Em sua primeira inicialização o componente `Entity Manager` gera seu próprio par de chaves para registrar sua própria identidade raiz na *blockchain*, a partir deste momento ele pode emitir novas identidades folha. Como a rede *blockchain* é mantida

[2] https://www.redhat.com/pt-br/topics/api/what-is-a-rest-api

por um consórcio de entidades administrativas, cabe aos administradores da rede conceder as permissão de escrita na *blockchain* ao componente `Entity Manager`. Assim, cada organização participante da rede (i.e., Entidades Administrativas do poder público) possui uma instância do `Entity Manager`, para emitir e revogar identidades para diversos contextos de aplicação. Em outras palavras, o componente `Entity Manager` representa as Entidades Administrativas e é capaz de executar os métodos implementados pelos contratos inteligentes. De forma colaborativa, os gestores de uma cidade podem utilizar muitas instâncias desse componente para implementar cenários do tipo: uma secretaria de transporte emitindo identidades para seus ônibus, enquanto uma secretaria de segurança pública emite identidades para suas câmeras de segurança.

Como cada identidade deve estar associada a um par de chaves criptográficas, convencionou-se que as chaves utilizadas por um dispositivo IoT devem ser geradas localmente no dispositivo, evitando a transmissão de chaves privadas pela *Internet*. Uma vez que o dispositivo tem seu par de chaves gerado, cabe ao administrador do `Entity Manager` registrar a identidade do dispositivo na *blockchain* associando à respectiva chave pública. Cada portador de identidade, ou administrador dos dispositivos, deve manter as chaves privada em segredo enquanto as componentes públicas são registradas na *blockchain*. Através das chaves criptográficas é possível utilizar as identidades digitais para identificação, autenticação mútua e garantir a procedência/integridade de dados. A Figura 18 ilustra o processo de geração de uma identidade pelo administrador do `EntityManager`, após a geração/instalação das chaves do dispositivo o administrador por executar a operação de (1) registro da identidade, após isso o próprio `EntityManager` utiliza sua chave privada para (2) gerar uma prova de sua identidade que então é (3) transmitida para contrato inteligente, que valida a identidade da entidade administrativa e registra a nova identidade folha para o ator.

Figura 18 – Processo de registro de novas Identidades.



Fonte: autoria própria.

4.4.2 IoT Cataloguer

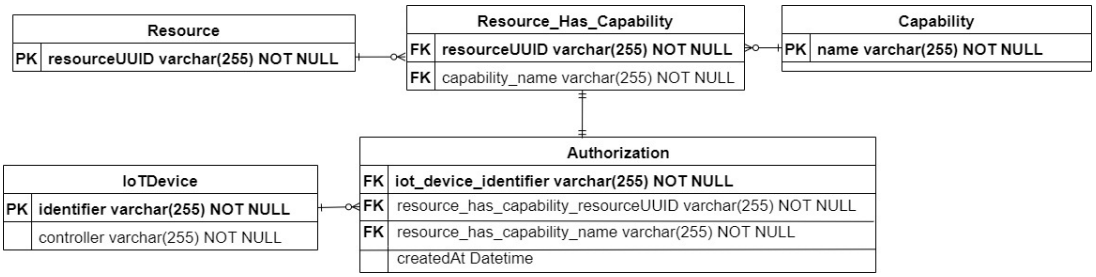
Para compreender melhor sobre o componente de *software* `IoT Cataloguer` devemos retomar alguns conceitos sobre a plataforma *InterSCity*. A Plataforma *InterSCity* facilita o desenvolvimento de aplicações de cidades inteligentes modelando a cidade em termos de recursos e capacidades. Na plataforma não existe o conceito do dispositivo IoT que de fato é o ator que coleta os dados e transmite para a plataforma, existem apenas recursos (e.g., ônibus inteligente) e capacidades (e.g., localização). Não existe qualquer diferenciação sobre as requisições de inserção de dados, em relação a qual dispositivo está enviando os dados para quais recursos. Dessa forma qualquer dispositivo poderia se passar por outro apenas informando na requisição o identificador do recurso.

O componente `IoT Cataloguer` é o responsável por estender o modelo de dados da plataforma *InterSCity* para considerar a existência dos dispositivos IoT que possuem identidade e considerar que os dispositivos identificados atuam em função de um recurso da cidade. Através dessa extensão, torna-se possível criar identidades para os dispositivos e atribuir permissões de acesso para garantir que apenas os dispositivos com autorização para aquele recurso e para aquelas capacidades podem inserir os dados de tal forma. Dessa forma, não é mais possível inserir dados na plataforma sem uma identidade para o dispositivo/*gateway* IoT sem autorização.

Isso é feito através de uma base de dados relacional que mapeia os endereços de identidade dispositivos existentes e seus controladores, qual o recurso da cidade aquele dispositivo representa e quais as capacidades que o dispositivo está autorizado a inserir dados. A Figura 19 apresenta o diagrama entidade relacionamento que modela o controle de admissibilidade implementado pelo `IoT Cataloguer`. Este componente possui integração com o `Entity Manager` de forma que as inclusões de autorizações são feitas a partir `Entity Manager`. Foram implementadas regras que garantem que apenas a Entidade Administrativa controladora da identidade do dispositivo é capaz de conceder as autorização. Antes do registro de autorizações o `Entity Manager` utiliza sua identidade para se autenticar com o `IoT Cataloguer`, que valida a identidade através de consultas a *blockchain*. O `IoT Cataloguer` permite que duas identidades sejam associadas em função de um mesmo recurso desde que sejam identidades emitidas por Entidades Administrativas diferentes. Este é o cenário onde um mesmo recurso da cidade (e.g., ônibus inteligente) possui dois dispositivos IoT provenientes de duas Entidades Administrativas que atuam em colaboração, por exemplo: uma secretaria de transporte instala um dispositivo transmissor de coordenadas e a secretaria de segurança instala câmeras de segurança. Nesse caso, os dois dispositivos conseguiriam compartilhar um mesmo recurso, porém não as mesmas capacidades. Além disso, também implementou-se uma restrição que impede que uma mesmo dispositivo portador de identidade seja relacionado a mais de um recurso, de forma a garantir que o dispositivo tem finalidade única para aquele recurso específico naquelas

capacidades específicas.

Figura 19 – Diagrama entidade relacionamento entre: dispositivos IoT, recursos, capacidades e autorizações.



Fonte: autoria própria.

4.4.3 Secure Resource Adaptor

O `Secure Resource Adaptor` é um extensão de um componente já existente no *InterSCity*. O component que foi estendido é chamado de `Resource Adaptor`, ele é o microsserviço da plataforma *InterSCity* responsável pela inclusão dos dados na plataforma. Para inserção de dados, é necessário enviar uma requisição para o `Resource Adaptor` especificando qual o recurso, qual a capacidade e o valor do dado. Por exemplo, um ônibus inteligente é um recurso representado na plataforma e a sua localização é uma de suas capacidades. Conforme já citado não há nenhum controle sobre que dispositivos podem inserir dados ou quais capacidades cada dispositivo está autorizado a publicar dados. Um dispositivo malicioso poderia se passar por outro simplesmente alterando o identificador do recurso na requisição de inserção de dados. Este controle é adicionado pelo `Secure Resource Adaptor`, que possui as mesmas atribuições do `Resource Adaptor` porém exige a autenticação do dispositivo antes de permitir requisições de inserção de dados. Além disso, o `Secure Resource Adaptor` é capaz de consultar o `IoTCataloguer` para recuperar as permissões dos dispositivos autenticados. Dessa forma, a plataforma através do `Secure Resource Adaptor` não está aberta para recepção indiscriminada de dados, apenas os dispositivo portadores de identidades e com permissões atribuídas no `IoTCataloguer` podem inserir dados na plataforma. As operações de autenticação são custosas pois envolvem consultas a *blockchain*. Para mitigar esse custo adotou-se o uso de *tokens JSON Web Token* (JWT) [3] como resultado das autenticações. Ao receber a mensagem de autenticação do dispositivo com uma prova de identidade, o `Secure Resource Adaptor` consulta a *blockchain* para validar a identidade do dispositivo e então consulta o `IoTCataloguer` para recuperar as permissões (i.e., qual recurso e capacidades o dispositivo está autorizado a acessar). Em posse dessas informações um *token* JWT é devolvido como resultado da autenticação. Este *token* deve ser mantido em segredo e nele estão contidas as permissões do dispositivo. A Figura 20 ilustra o modelo de dados que compõe o *token*, nele estão

[3] https://datatracker.ietf.org/doc/html/rfc7519

presentes o identificador da identidade do dispositivo na *blockchain* (**sub**), assinatura que comprova que o *token* foi emitido pelo `SecureResourceAdaptor`, as permissões de acesso do dispositivo (**permissions**) que é composta pelo *Universal Unique Identifier* (UUID) do recurso e pela lista de capacidades permitidas, e a data de validade do *token* (**exp**).

Figura 20 – Estrutura do *token* recuperado pelo dispositivo como resultado da autenticação.


```
{
  "sub": "dispositivo:iot:onibus-inteligente",
  "sig": "eyJraWQiOiJzc3A6ZG ... bkumexZ0VJBkJHyU30UN4ZO36ZA",
  "permissions": {
    "resourceUUID": "dfde8ff0-d224-4aab-83e3-a8386ccb7eaf",
    "capabilities": [
      "localização",
      "imagens-camera"
    ]
  },
  "admin": false,
  "exp": 1720313423
}
```


Fonte: autoria própria.

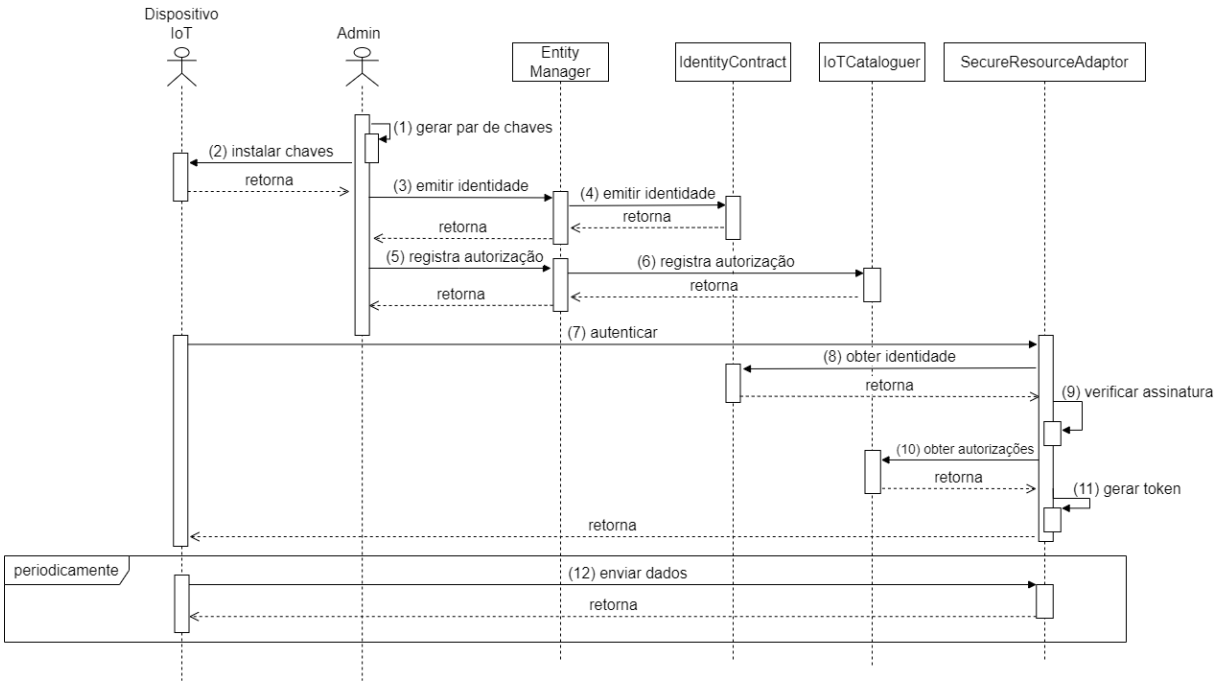
A inserção de dados por meio do `Secure Resource Adaptor` requer o *token* e a partir do *token* são extraídos as permissões e então o dado apenas é inserido caso as permissões sejam adequadas. O *token* possui validade parametrizável que pode ser configurado para durar o tempo que for necessário de acordo com o contexto de aplicação. Dessa forma, a autenticação não precisa ocorrer de forma tão frequente e assim pode-se economizar recursos computacionais.

A Figura 21 apresenta o diagrama de sequência que descreve o fluxo sequêncial que ilustra todo o processo desde a geração de chaves criptográficas até a inserção de dados na plataforma *InterSCity*. Inicialmente o administrador (1) gera e (2) instala o par de chaves do dispositivo, e então (3) requisita ao `Entity Manager` a emissão da identidade que é (4) registrada na *blockchain* por meio do contrato inteligente. Após isso são (5,6) concedidas as autorizações do dispositivo e a partir desse ponto o dispositivo pode se (7) autenticar com o `Secure Resource Adaptor` que obtém a identidade (8) para a (9) validação. Após a validação da identidade, o `Secure Resource Adaptor` (10) requisita ao `IoTCataloguer` as permissões da identidade associada ao dispositivo que são (1) codificadas no *token*. Após obtenção do *token* o dispositivo consegue inserir os dados na plataforma *InterSCity* por meio do `Secure Resource Adaptor`.

4.5 Comparação com Trabalhos Relacionados

Após a especificação do modelo de gestão de identidade, escrita dos contratos inteligentes, implementação dos componentes de *software* e da integração com a plataforma

Figura 21 – Diagrama de sequência correspondente ao processo de registro de dispositivos, autenticação e envio de dados a plataforma InterSCity.



Fonte: autoria própria.

InterSCity, retoma-se a discussão a cerca dos trabalhos relacionados com a inclusão da solução proposta. A Tabela 3 retoma o quadro comparativo do capítulo anterior com a adição da solução proposta.

Tabela 3 – Comparação de Trabalhos Relacionados

Trabalho	**Escal.**	**Dispon.**	**Gov.**	**Descen.**	**Impl.**	**CI**
(BOURAS *et al.*, 2021)	Sim	Sim	Sim	Sim	Sim	Não
(OMAR; BASIR, 2018)	Parcial	Sim	Sim	Semi	Parcial	Não
(CHEN; LIU; CHAI, 2015)	Sim	Sim	Não	Sim	Não	Não
(VENKATRAMAN; PARVIN, 2022)	Parcial	Sim	Sim	Não	Sim	Não
(WANG *et al.*, 2022)	Sim	Sim	Sim	Sim	Sim	Não
Solução Proposta	Sim	Sim	Sim	Sim	Sim	Sim

O modelo proposta nesta dissertação satisfaz os critérios utilizados para comparação dos trabalhos relacionados. Em relação a escalabilidade, a solução proposta utiliza três *ledgers* separados para as operações de emissão de identidades, revogação de identidades e registro de autenticações. Esta estratégia permite que as operações sejam feitas de forma independente em *ledgers* distintos. Isto permite que um fluxo alto de transações de um tipo interfira no tempo de resposta dos outros tipos transações e também permite a execução em paralelo das operações. Além disso, mostrou-se que é possível utilizar *tokens* de validade configurável para diluir a quantidade de operações de autenticações que precisem ser feitas por um mesmo dispositivo, o que contribui para o aumento do número de dispositivos capazes de usar o modelo de forma simultânea. Os critérios de disponibilidade e governança

também são satisfeitos através do uso da tecnologia *blockchain*. Como a *blockchain* é uma rede distribuída não existe apenas um ponto central a partir do qual são efetuadas as operações, de forma que problemas de pontos únicos de falha são mitigados. Para garantir uma governança transparente, aproveitou-se a *blockchain* permissionada *Hyperledger Fabric*. No modelo proposto as Entidades Administrativas precisam consentir com os contratos inteligentes estabelecidos e contribuir com a manutenção da rede, além disso o ingresso de novas entidades está sujeito a aprovação das demais. A descentralização também é um critério atendido, uma vez que todas as Entidades Administrativas tem as mesmas atribuições e capacidades de gestão de identidades de forma independente uma das outras. Não é possível uma Entidade revogar identidade emitida por outra Entidade, assim como não é possível negar a procedência das identidades emitidas. Em relação a implementação do modelo, foi possível demonstrar a flexibilidade e aplicabilidade do modelo de gestão de identidades proposto a partir da integração com uma plataforma de CI já existente. A plataforma *InterSCity* não possuía nenhuma forma de autenticação e controle sobre os dados que eram inclusos nela. Foi possível desenvolver tais funcionalidades utilizando nosso modelo de forma estender a plataforma sem precisar fazer qualquer alteração no código fonte da plataforma.

De maneira geral a solução proposta se destaca das demais por oferecer um modelo de gestão de identidades flexível e voltado para o contexto de CI, incluindo todos os eventuais atores existentes em uma cidade com exceção do cidadão. Assim como a solução proposta nesta dissertação, outros dois trabalhos também satisfazem todos os critérios. Em (BOURAS *et al.*, 2021) é apresentado um modelo de gestão de identidades similar ao proposto, apesar disso a solução proposta se destaca por se capaz de incluir mais atores além dos dispositivos IoT e aplicações IoT. A flexibilidade do modelo proposto para identificar quaisquer atores da cidade foi demonstrada através da integração com a plataforma *InterSCity*. O modelo proposto também se destaca em relação ao processo de autenticação, pois em (BOURAS *et al.*, 2021) o processo a autenticação deve ocorrer toda vez que uma entidade interage com outras entidades, enquanto no modelo proposto foram utilizados *tokens* JWT para permitir que a autenticação ocorra apenas uma vez e tenha duração parametrizável. Em (WANG *et al.*, 2022) também estão satisfeitos todos os requisitos, a solução proposta se destaca pois tem como foco identificar atores existentes em uma CI e oferecer mecanismos para difundir a segurança através de identidades digitais, enquanto (WANG *et al.*, 2022) aborda uma solução para resolver problemas puramente de IoT relacionadas ao grande volume de dispositivos conectados, e suas limitações em termos de recursos computacionais, e da grande quantidade de dados coletados. Em (CHEN; LIU; CHAI, 2015) foi proposto um modelo informacional e protocolos para a gestão de identidades. A solução proposta se destaca pois além disso também faz uma implementação do modelo e integração com uma plataforma de CI já existente. Em relação a (VENKATRAMAN; PARVIN, 2022) a solução proposta de diferencia pois

aborda o contexto de uma CI composta por diversas Entidades Administrativas que de forma colaborativa podem participar do processo de gestão das identidades dos atores da cidade, enquanto em (VENKATRAMAN; PARVIN, 2022) o trabalho é limitado a gestão de identidades de dispositivos de uma única organização. Em relação ao trabalho apresentado por (OMAR; BASIR, 2018), a solução proposta destaca-se pois o próprio autor classifica seu modelo como semi-descentralizado e não apresenta considerações a certa da escalabilidade do modelo proposto.

5 Avaliação Experimental

Neste capítulo será conduzida uma avaliação experimental que possui o objetivo de avaliar os impactos da adoção do modelo proposto. Para isso, utilizou-se cenários de testes que simulam aplicações desenvolvidas no contexto de Cidades Inteligentes que utilizam a plataforma *InterSCity* para publicação de dados. Ao todo foram realizados três experimentos distintos mas que utilizam a mesma abordagem para a avaliação. Cada cenário de testes foi reproduzido duas vezes, a primeira utilizando da solução proposta que inclui os canais seguros de comunicação com mecanismos de autenticação, controle de acesso e confidencialidade (i.e., *Transport Layer Security* (TLS)), e a segunda com as comunicações sendo feitas diretamente com a plataforma InterSCity sem quaisquer mecanismos de segurança.

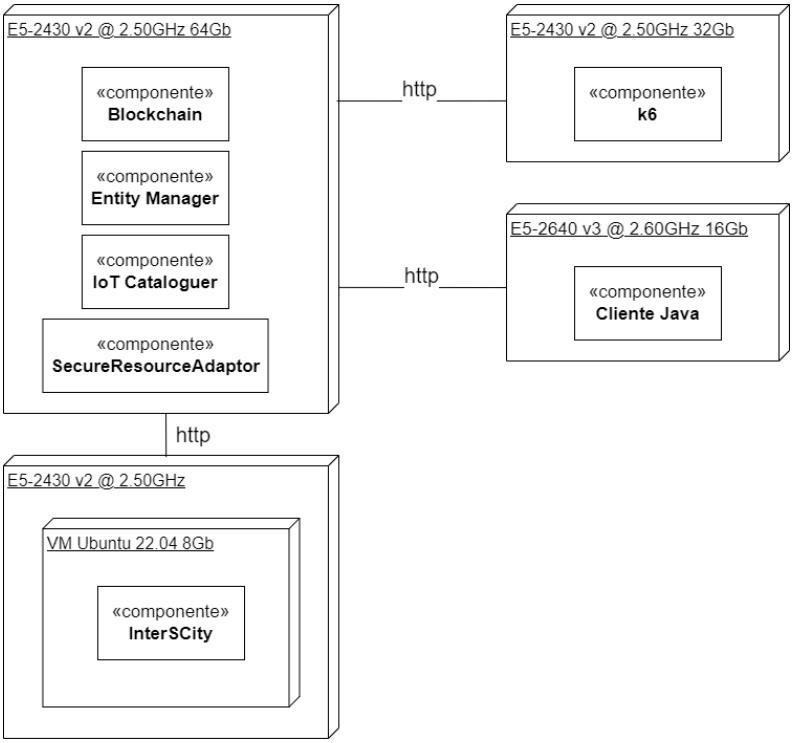
5.1 Ambiente de Execução

Todos os experimentos foram executados através de três servidores, uma máquina virtual e uma estação de trabalho. Os experimentos são executados através clientes virtuais que fazem requisições periódicas. Os dois primeiros experimentos utilizam clientes simulados através de uma ferramenta de testes chamada *k6*[1]. O terceiro experimento simula os clientes através de uma aplicação *Java* que foi implementada especialmente para o experimento. A simulação de clientes em duas formas foi feita devido as facilidades de cada forma para a coleta das métricas. As configurações de cada servidor e suas atribuições no contexto do experimento serão apresentados a seguir. O ambiente de execução é representado a partir do diagrama de *deployment* presente na Figura 22.

O primeiro servidor, com processador *E5-2430 v2 @ 2.50GHz* e 64 *Gigabyte* (Gb) de memória *Random Access Memory* (RAM), foi utilizado exclusivamente para para rodar os componentes de *software* que compõe a solução proposta: `Entity Manager`, `IoT Cataloguer`, `Secure Resource Adaptor` e a rede *blockchain*. O segundo servidor, que possui o mesmo processador do anterior porém com 32 Gb de RAM, foi utilizado de forma dedicada para executar a ferramenta de testes *k6*. A máquina virtual *ubuntu 22.04*, de 8 Gb de RAM foi dedicada exclusivamente para rodar a plataforma *InterSCity* composta por seus microsserviços, esta máquina virtual roda em um terceiro servidor de configuração semelhante os anteriores. Por fim uma estação de trabalho *E5-2640 v3 @ 2.60GHz 2.60 GHz* com 16 Gb de RAM foi utilizada para hospedar os clientes de teste implementados na linguagem *Java*.

[1] https://k6.io/docs/

Figura 22 – Diagrama de *deployment* que ilustra o ambiente de execução.



Fonte: autoria própria.

5.2 Latência nas Operações de Autenticação

Neste experimento considera-se um cenário de aplicação hipotético no contexto de CI, neste cenário a administração de uma Cidade Inteligente dispõe de 150 veículos para distribuição de cargas no qual em cada veículo está instalado um dispositivo IoT ou *gateway* capaz de transmitir periodicamente as coordenadas do veículo para a plataforma *InterSCity*. Estes dados são consumidos diretamente da plataforma pela central de logística que dispõe de um *dashboard* que mostra em tempo real as localizações dos veículos e os destinos de cada um. Com esse serviço é possível coletar métricas relativas ao tempo de entrega, calcular as melhores rotas e analisar a efetividade das operações logisticas de entrega.

No primeiro experimento, tentou-se reproduzir este cenário descrito utilizando a solução proposta no qual os dispositivos que coletam e publicam o dado são identificados com identidades emitidas pela entidade administrativa (e.g., secretaria de planejamento) e precisam se autenticar com o `Secure Resource Adaptor` antes de publicar os dados de forma segura na plataforma *InterSCity*. O objetivo do experimento é avaliar o tempo de latência para as operações de autenticação de dispositivos com o `Secure Resource Adaptor`.Para isso, utilizou-se a ferramenta *k6* para simular 150 clientes enviando as requisições de autenticação periodicamente. Configurou-se a ferramenta para que o experimento durasse aproximadamente 10 minutos, com o número máximo de clientes configurado em 150. Durante os primeiros dois minutos, o número de clientes aumenta gradualmente de 0

até atingir 150 onde se estabiliza por 5 minutos. Por fim, nos últimos dois minutos o número de clientes diminui até retornar a 0. A frequência de envio de requisições de autenticação foi definida como uma requisição a cada um segundo. Esta frequência foi escolhida de forma a estressar a solução proposta uma vez que o *token* obtido na autenticação tem validade configurável e em cenários reais teria validade muito superior a um segundo. Durante a execução do experimento, foram coletados os valores da latência das requisições de autenticação executadas pelos clientes virtuais. Para a representação gráfica dos resultados, utilizou-se a linguagem *Python* e a biblioteca *Pandas*.

5.2.1 Resultados Obtidos

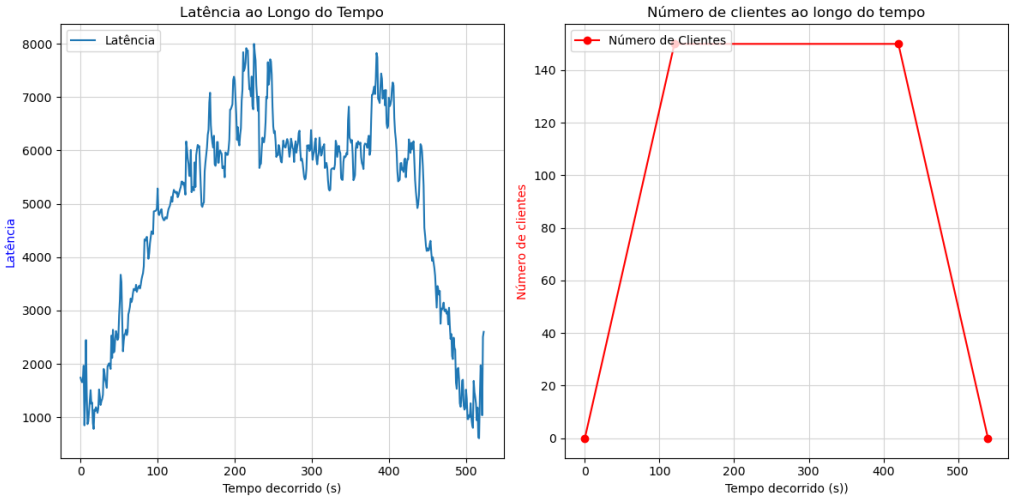
A tabela 8 apresenta as estatísticas básicas do valor da latência das operações de autenticação. Ao todo foram executadas 10564 requisições ao longo de aproximadamente 10 minutos, o que totaliza em média 19 transações por segundo. A figura 23 apresenta o gráfico dos valores de latência e latência acumulada ao longo do tempo.

Tabela 4 – Média, mediana, moda e percentis da latência das requisições de autenticação de dispositivo com a plataforma *InterSCity*

Estatística	**Valor (ms)**
Numero de requisições	10564
Média	4998
Desvio padrão	1774
Min	513
25%	3846
50% (Mediana)	5665
75%	6129
Max	8430

No primeiro experimento, tentou-se reproduzir o cenário no qual diversos dispositivos IoT pertencente as entidades administrativas da cidade executam operações de autenticação com o `Secure Resource Adaptor` com o objetivo avaliar o tempo de latência para as operações de autenticação de dispositivos com o `Secure Resource Adaptor`. Ao observar os resultados, verifica-se que ao longo de 10 minutos foram executadas 10564 requisições de autenticação, totalizando aproximadamente 19 transações por segundo. O padrão observado na figura 23 mostra que a latência aumenta conforme o número de usuários também aumenta, e que ao reduzir a carga de usuários a latência volta a diminuir. Este comportamento é o esperado, e indica que a aplicação consegue retornar ao estado inicial. A média do tempo para efetuar uma autenticação ficou em aproximadamente 5 segundos, esta operação é custosa, uma vez que a autenticação é feita através do par de chaves criptográficas e o resultado desta autenticação é armazenada na *blockchain* por meio de uma transação. Apesar deste valor ser relativamente alto isso não é um impeditivo para

Figura 23 – Latência (ms) e número de clientes virtuais ao longo do tempo, para as operações de autenticação. Fonte: Autoria própria.



Fonte: autoria própria.

uso da solução proposta. Uma cidade inteligente não possui recursos infinitos, e portanto, não haverão dispositivos ilimitados se autenticando, além disso, a autenticação utiliza um modelo baseado em *tokens* que possuem validade configurável, sendo possível distribuir a quantidade de dispositivos se autenticando ao longo do tempo. Considerando os resultados obtidos, com taxa de 19 transações de autenticação por segundo, em um dia é possível realizar 1.641.600 operações de autenticação, ou 68.400 autenticações por hora. Com estes valores é possível atender dispositivos provenientes de diferentes tipos de aplicações que possuem diferentes necessidades. Por um lado existem dispositivos que atuam em operações críticas e necessitam se autenticar com mais frequência, mas também existem aqueles que não necessitam se autenticar com frequência. Ao aumentar a validade do *token*, pode-se diluir a quantidade de dispositivos se autenticando no mesmo momento, e isto pode ser aproveitado para compensar os dispositivos que autenticam-se com mais frequência. Ao configurar a validade do *token* torna-se possível atender diversos dispositivos no contexto de IoT e CI.

5.3 Latência na Inserção de Dados na Plataforma InterSCity

Seguindo o mesmo contexto do exemplo anterior, neste experimento reproduziu-se o cenários os onde 150 dispositivos transmitem suas coordenadas periodicamente para a plataforma *InterSCity*. O objetivo deste experimento é avaliar a latência das operações de inserção de dados a plataforma *InterSCity* através da comparação entre a inserção dos dados utilizando o modelo proposto que inclui os canais seguros de comunicação com mecanismos de autenticação, controle de acesso e confidencialidade (i.e., TLS) e a inserção de dados diretamente na plataforma *InterSCity*, onde não existem mecanismos

de segurança. Para isso, utilizou-se a ferramenta *k6*, para simular 150 clientes enviando requisições de inserção de dados na plataforma *InterSCity*. Configurou-se a ferramenta para que o experimento durasse aproximadamente 10 minutos com o número máximo de clientes configurado para 150. Durante os primeiros dois minutos, o número de clientes aumenta gradualmente de 0 até atingir 150 onde se estabiliza por 5 minutos. Por fim, nos últimos dois minutos o número de clientes diminui até retornar a 0. A frequência de envio de requisições foi definida como 1 requisição a cada 10 segundos. Na primeira etapa, aplica-se o modelo de gestão de identidades proposto para que clientes virtuais possuidores de identidades insiram dados de forma segura na plataforma *InterSCity*, através do `Secure Resource Adaptor`. Na segunda etapa, os dados foram inseridos diretamente na plataforma utilizando o componente `Resource Adaptor`, já existente na plataforma *InterSCity* e sem quaisquer mecanismos de segurança. Durante a execução do experimento, foram coletados os valores da latência das requisições de inserção de dados feitas pelos clientes virtuais. Para a representação gráfica dos resultados, utilizou-se a linguagem *Python* e a biblioteca *Pandas*.

5.3.1 Resultados Obtidos

A Tabela 5 e tabela 6, apresentam respectivamente as estatísticas básicas relativas a latência das requisições de inserção de dados submetidas diretamente à plataforma *InterSCity*, e as requisições submetidas utilizando o modelo proposto juntamente com o `Secure Resource Adaptor`. Como as métricas foram coletadas de clientes virtuais que executam em paralelo, houveram muitos valores registrados com o mesmo horário, impossibilitando uma plotagem direta dos gráficos. Para tratar esta situação, agrupou-se as leituras registradas no mesmo horário e tomou-se como valor a média dos valores agrupados.

Tabela 5 – Dado inserido diretamente

Estatística	**Valor (ms)**
Contagem	533
Média	23
Desvio padrão	43
Min	9
25%	13
50% (Mediana)	14
75%	19
Max	818

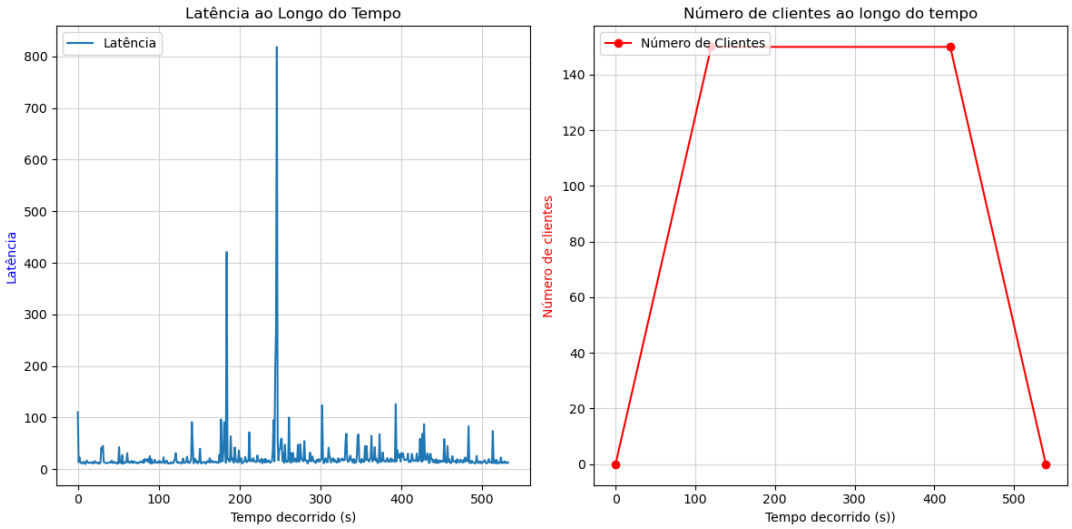
Tabela 6 – Dado inserido via *Secure Resource Adaptor*

Estatística	**Valor (ms)**
Contagem	520
Média	473
Desvio padrão	591
Min	14
25%	24
50% (Mediana)	258
75%	783
Max	6167

A Figura 24 apresenta os gráficos que representam, respectivamente, a média da latência das requisições ao longo do tempo e a quantidade de clientes ao longo do tempo,

enviando as requisições diretamente para a plataforma *InterSCity* sem o estabelecimento de canais seguros de comunicação.

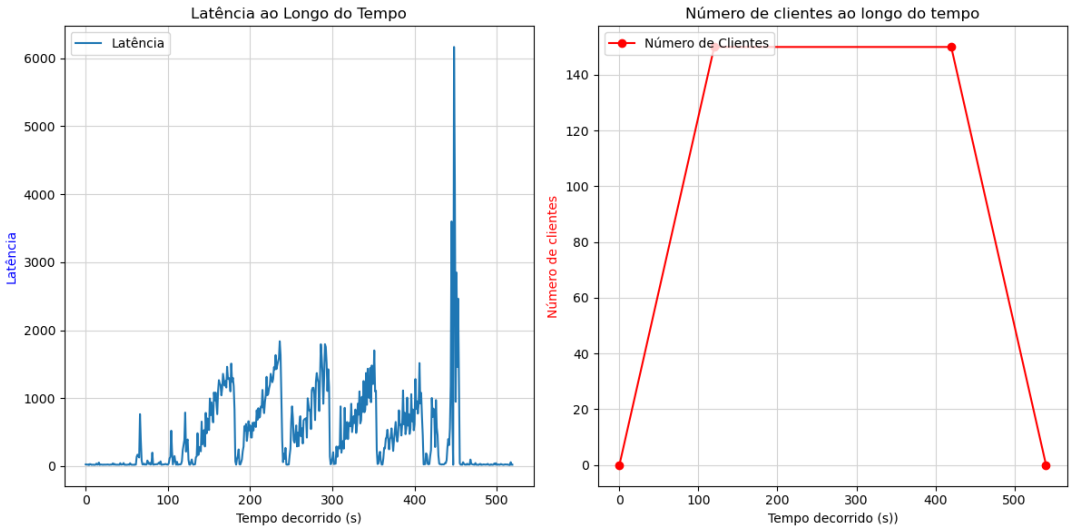
Figura 24 – Latência (ms) e número de clientes ao longo do tempo, inserindo os dados diretamente no *InterSCity*.



Fonte: autoria própria.

A Figura 25 apresenta os gráficos que representam, respectivamente, a média da latência das requisições ao longo do tempo e a quantidade de clientes ao longo do tempo ao se enviar as requisições através do `Secure Resource Adaptor`, com os mecanismos de autenticação, controle de acesso e estabelecendo canais seguros de comunicação.

Figura 25 – Latência (ms) e número de clientes ao longo do tempo, utilizando o modelo proposto.



Fonte: autoria própria.

Os resultados obtidos mostram que a latência das requisições de inserção de dados são menores quando inserimos os dados diretamente na plataforma. Isto ocorre

pois a plataforma não possui funcionalidades de autenticação e controle de acesso, estas funcionalidades foram introduzidas ao integrar o modelo proposto com a plataforma *InterSCity*. Estas funcionalidades a mais justificam o aumento da latência ao inserir os dados utilizando o modelo proposto. O aumento é aparentemente alto, passando de 23 milissegundos para 473 milissegundos ao adotar. Apesar disso, esta variação na realidade tende a ser menor pois a plataforma *InterSCity* possui mecanismos nativos para balanceamento de carga e o componente `Secure Resource Adaptor` da solução proposta foi integrada como um serviço a parte, não fazendo uso desses mecanismos nativos. Portanto a tendência é que esse valor seja menor. Além disso, em cenários reais, a frequência de atualização dos dados é definida de acordo com o domínio de aplicação e assim nem todas as aplicações precisam ter frequências altas para a atualização dos dados. Dessa forma, nossa solução consegue atender às diversas aplicações que produzem dados. Neste experimento, considerou-se apenas uma instância da plataforma *InterSCity* e apenas uma instância do `Secure Resource Adaptor`, em cenários reais pode-se aumentar sob demanda a quantidade de instâncias dos microsserviços da plataforma e também do `Secure Resource Adaptor`, aumentando-se assim a escalabilidade do modelo proposto em relação a capacidade de recepção de dados provenientes de dispositivos IoT.

5.4 Consumo de Memória e Processamento por Clientes

Neste último experimento, considerou-se outro cenário que leva em conta apenas um dispositivo IoT e tem como objetivo avaliar o custo computacional em termos de consumo de memória e processamento para um dispositivo da cidade que utilize a solução proposta. Podemos tomar como exemplo o diapositivo IoT ou *gateway* presentes nos veículos de entrega do exemplo citado anteriormente. Como o modelo proposto adiciona funcionalidades de segurança é necessário entender os custos da adoção da solução. Para isso, foi desenvolvida uma aplicação *Java* que simula um cliente/dispositivo que envia periodicamente suas coordenadas para a plataforma *InterSCity*. A aplicação foi programada para enviar requisições de inserção de dados à plataforma *InterSCity* com um intervalo de 100 milissegundos entre cada requisição. Utilizou-se a ferramenta *Your Kit* para coleta das métricas de desempenho de aplicações *Java*.

O experimento teve uma duração total de aproximadamente 10 minutos, durante os quais a aplicação simuladora do dispositivo enviou dados de forma contínua para a plataforma. O experimento foi dividido em duas fases distintas. A primeira com o uso da solução proposta através dos canais seguros de comunicação que incluem os mecanismos de autenticação, controle de acesso e confidencialidade (i.e.,TLS), e o segundo comunicando diretamente com a plataforma InterSCity sem quaisquer mecanismos de segurança. Durante a execução do experimento, foram coletados dados sobre o consumo de memória e processamento da aplicação. Após a conclusão do experimento, as estatísticas

básicas dos dados coletados foram calculadas, e os valores de consumo de memória e processamento foram plotados em gráficos para facilitar a visualização e análise comparativa entre as duas fases do experimento. Para a representação gráfica dos resultados, utilizou-se a linguagem *Python* e a biblioteca *Pandas*.

5.4.1 Resultados Obtidos

Os resultados obtidos deste experimento são apresentados na tabela 7 e tabela 8, que mostram respectivamente as estatísticas básicas do consumo de memória RAM para um dispositivo IoT. As tabelas 9 e tabela 10, apresentam as estatísticas básicas do consumo de processamento, em termos de percentual do total disponível, para um dispositivo virtual. A partir dos dados coletados, observa-se que há um custo adicional para um eventual dispositivo IoT em adotar-se o modelo proposto para inserção de dados de forma segura na plataforma *InterSCity*. Este custo adicional pode ser percebido tanto em relação ao uso de memória RAM quando em uso de processamento.

Tabela 7 – Consumo de memória RAM não utilizando o modelo

Estatística	**Valor (Mb)**
Nº de Medições	743
Média	29,94
Desvio padrão	22,85
Min	3,48
25%	11,48
50% (Mediana)	23,96
75%	41,96
Max	83,96

Tabela 8 – Consumo de memória RAM utilizando o modelo proposto

Estatística	**Valor (Mb)**
Nº de Medições	751
Média	77,41
Desvio padrão	42,04
Min	7,47
25%	40,39
50% (Mediana)	77,02
75%	114,49
Max	153,86

Tabela 9 – Consumo de processamento não utilizando o modelo

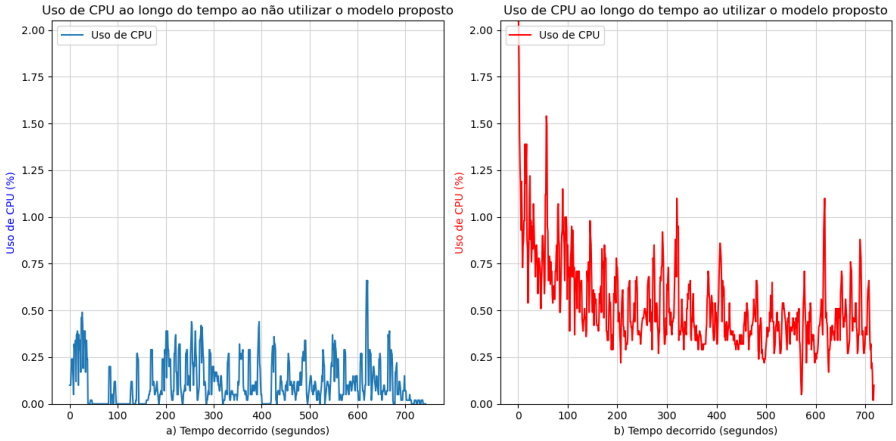
Estatística	**Valor (%)**
Nº de Medições	743
Média	0.,
Desvio padrão	0.11
Min	0,00
25%	0,02
50% (Mediana)	0.07
75%	0,19
Max	0,66

Tabela 10 – Consumo de processamento utilizando o modelo proposto

Estatística	**Valor (%)**
Nº de Medições	718
Média	0,52
Desvio padrão	0,23
Min	0,02
25%	0,37
50% (Mediana)	0,46
75%	0,65
Max	2,05

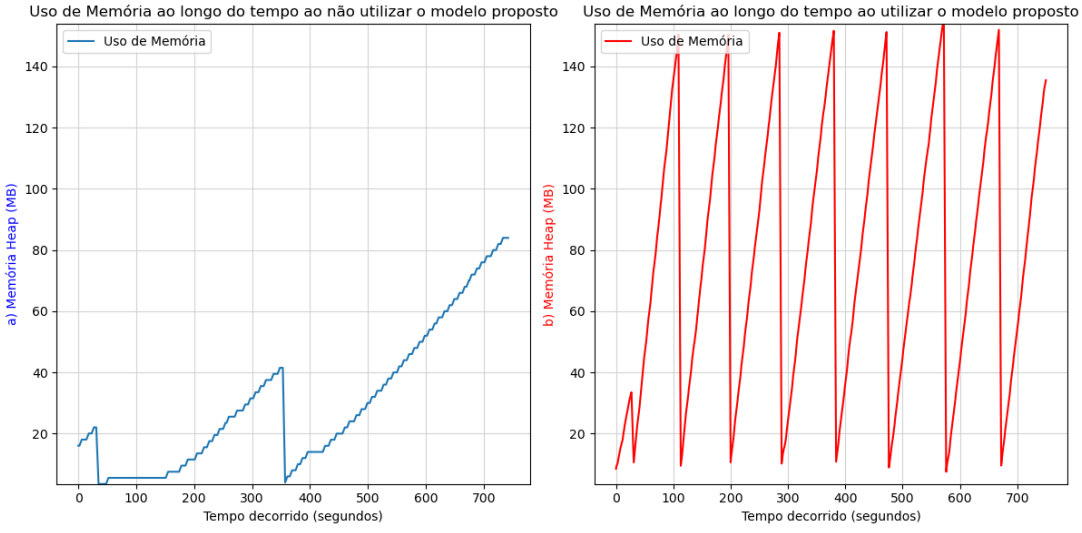
A figura 26 exibe um gráfico com os valores do uso de processamento ao longo do tempo, em percentual da capacidade total do sistema (i.e., 100%), por parte da simulação de dispositivo ao utilizar-se o modelo proposto e ao não utilizar o modelo. A figura 27 exibe os valores do uso de memória RAM ao longo do tempo, em *Megabyte* (Mb), por parte da simulação de dispositivo ao utilizar-se o modelo proposto e ao não utilizar o modelo.

Figura 26 – Consumo de processamento ao longo do tempo ao utilizar e ao não utilizar o modelo proposto.



Fonte: autoria própria.

Figura 27 – Consumo de memória ao longo do tempo ao utilizar e ao não utilizar o modelo proposto.



Fonte: autoria própria.

Conforme observado nos resultados, existe um custo adicional de memória e de processamento para o dispositivo ao utilizar a solução proposta. Percentualmente a variação dos valores é alta, mas em termos absolutos a adição de custo é baixa. A média de consumo de memória em Mb passa de aproximadamente 30 para 77, enquanto o processamento

passa de 0,1% da capacidade total para 0,52%. Existe uma troca, onde perde-se um pouco de desempenho para garantir a segurança. A partir do gráfico, percebe-se que o uso de memória por parte da aplicação não apresenta vazamentos de memória, de forma que os objetos alocados são liberados corretamente pelo *Garbage Collector* [2] (i.e., o gerenciador de memória do Java) quando deixam de ser utilizados. Este custo computacional adicionado ao dispositivo é baixo em valores absolutos e pode ainda ser reduzido em cenários reais a partir da utilização de *gateways* IoT de forma que vários dispositivos compartilhem o mesmo *gateway* para publicação dos dados. Dessa forma o aumento no custo computacional é aplicado apenas a um *gateway* que atua em função dos dispositivos IoT (e.g., uma ambulância equipada com um gateway e três sensores).

5.5 Discussão

Neste capítulo foram executados três experimentos com o objetivo de avaliar a solução proposta para fazer uma análise acerca do custo computacional e aplicabilidade da solução em ambientes de cidades inteligentes. O primeiro experimento avaliou a latência das operações de autenticação de dispositivos utilizando o modelo proposto. O segundo experimento avaliou a latência da inserção de dados na plataforma *InterSCity* utilizando o modelo proposto para garantir a procedência dos dados. E o terceiro experimento avaliou o custo de memória e processamento para um dispositivo portador de identidade que transmite dados periodicamente à plataforma *InterSCity*. De maneira geral, os resultados dos três experimentos mostram que existe um custo em termos de uso de processamento e memória ao adicionar uma camada de segurança baseada no modelo proposto. Este custo era esperado, uma vez que ao adotar o modelo são feitas mais operações para garantir a segurança. A partir dos cenários hipotéticos considerados, mostra-se que a solução é aplicável ao contexto de CI, que não possui recursos infinitos e geralmente conta com dinheiro público. Por exemplo, o número de transações de autenticações por segundo atingido durante o experimento mostra que é possível atender um grande número de dispositivos presentes em uma cidade, e que em cenários de aplicação reais este número tende a ser maior. Ao definir uma validade para o *token* aumentamos ainda mais a quantidade de dispositivos que podem se autenticar ao longo do tempo, além disso também torna-se possível economizar recursos da cidade ao diminuir a quantidade de operações executadas.

[2] https://www.oracle.com/webfolder/technetwork/tutorials/obe/java/gc01/index.html

6 Conclusão

Conforme os objetivos especificados inicialmente, neste trabalho foi proposto um modelo para gestão descentralizada de identidades voltado para IoT e CI utilizando a tecnologia *blockchain*. Inicialmente especificou-se o modelo de gestão de identidades e então implementou-se o modelo por meio de contratos inteligentes que executam na *blockchain Hyperledger Fabric*. Também foram desenvolvidos os componentes de *software* para facilitar a utilização do modelo (i.e.,`Entity Manager`) e dos componentes de *software* para integração do modelo com a plataforma *InterSCity* no intuito de adicionar funcionalidades de autenticação, e controle de acesso para dispositivos IoT, assim como estabelecimento de canais seguros de comunicação. Tais funcionalidades de segurança não existiam anteriormente no *InterSCity*, o que impedia seu uso em cenários de aplicação reais. Após o desenvolvimento da solução proposta foi possível integrar o modelo desenvolvido para garantir que apenas os dispositivos corretos sejam capazes de se autenticar a plataforma para inserção de dados de IoT e também garante-se um controle de acesso para os dispositivos baseado nos recursos e capacidades da plataforma *InterSCity*. Isto é feito por meio dos componentes de *software* implementados (i.e.,`IoTCataloguer` e `Secure Resource Adaptor`). O uso de *blockchain* para armazenar as identidades dos atores de uma CI favorece a criação de um ambiente compartilhado entre entidades administrativas, que são capazes de gerir de forma independente as identidades dos demais atores. O fato de serem usados contratos inteligentes para gerir identidades, faz com que o comportamento da solução seja público, de forma que os participantes (i.e., entidades administrativas) devem concordar com os termos de antemão. Ao usar *blockchain* nosso modelo elimina pontos únicos de falha, uma vez que os dados são mantidos em diferentes nós, e também aumenta-se a disponibilidade das informações de identidade. Não é possível apagar os registros do livro-razão, de forma que a todo momento pode-se recuperar todas as operações que ocorreram a caráter de validação, auditoria e responsabilização. Ao usar uma *blockchain* permissionada, os participantes da rede (i.e, entidades administrativas e demais atores) são previamente autorizados para escrita/leitura dos dados. Esta característica é adequada para ambientes de CI, onde os gestores tem o dever de responsabilidade para com os recursos da cidade que são públicos e devem ser tratados com o devido respeito. Portanto, além de resolver os problemas de um sistema de gestão de identidades centralizado, também propôs-se um sistema que pode facilmente ser aplicado em ambientes de CI, isso foi demonstrado com a integração com a plataforma *InterSCity*. Além disso, o modelo é genérico o bastante para ser aplicado a qualquer contexto de aplicação que requer identificação de participantes de uma cidade de forma descentralizada. Na discussão dos experimentos realizados, demonstra-se que apesar dos custos de implementação do modelo é possível implementa-lo para prover um

ambiente seguro para todas as entidades administrativas e demais atores existentes em uma cidade inteligente.

6.1 Limitações

Como limitações do trabalho, podemos citar o fato do modelo proposto não possuir suporte para identificação dos cidadãos de uma cidade. Os cidadãos são parte fundamental da cidade e também necessitariam de identificação para poder consumir os serviços da cidade. Apesar de não haver limitações técnicas pra emissão de identidades para cidadãos, isto não é considerado no modelo proposto pois existem diversos problemas relacionados a privacidade e exposição de dados pessoais do cidadão. Como estes problemas não foram abordados na solução considera-se que o modelo de gestão de identidades não deve ser utilizado para identificar os residentes da cidade. Além disso, a administração da rede por parte das entidades administrativas requer um significativo esforço em termos de administração da infraestrutura *blockchain*. Esta administração requer conhecimentos muitos específicos que possuem uma curva de aprendizagem longa. Apesar disso, o modelo pode ser aplicado em cidades inteligentes dedicando-se algum esforço neste sentido.

6.2 Trabalhos Futuros

Como trabalhos futuros, podemos incluir a adição de novas funcionalidades de segurança para a plataforma *InterSCity*. O modelo proposto foi utilizado para adicionar uma camada de segurança para inserção de dados de dispositivos na plataforma, porém não há autenticação e controle de acesso para o consumo de dados na plataforma. Isto é possível de ser feito também utilizando o modelo proposto e seus contratos inteligentes. Também não estão inclusos em nosso trabalho identidades voltadas para cidadãos. Este caso requer especial atenção, pois lida com dados pessoais e sensíveis, o que acarretaria em uma série de outras preocupação relacionadas a privacidade e divulgação de dados. Este novo ator introduz maior complexidade ao modelo já existente e portanto não foi considerado ainda. Para adição deste ator, espera-se investigar o uso de identidades auto soberanas para incluir o cidadão de forma a resguardar seus dados. Outra linha em que pode-se avançar futuramente, é o uso de técnicas *off-chain* [1], que são mecanismos para manter dados *offline* em paralelo com uma rede *blockchain* com objetivo de aumentar a velocidade e eficiência de custo, e escalabilidade em relação ao número de transações.

[1] https://www.coinbase.com/pt-br/learn/tips-and-tutorials/onchain-vs-offchain-cryptocurrency-transactions-what-is-the-difference

6.3 Publicações

Os resultados preliminares deste trabalho foram publicados no XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG). Além disso, está em processo de elaboração um artigo para publicação em periódico, o qual apresentará a versão final e consolidada desta pesquisa, contemplando todas as melhorias e resultados obtidos ao longo do estudo.

1. Gerenciamento Descentralizado de Identidades para Cidades Inteligentes Baseado na Tecnologia Blockchain (CARDOSO *et al.*, 2022). SBSEG. DOI: <https://doi.org/10.5753/sbseg.2022.224099>

Referências

AHMED, M. R. *et al.* Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *IEEE Access*, v. 10, p. 113436–113481, 2022. Citado na página 33.

ALAMER, M.; ALMAIAH, M. A. Cybersecurity in smart city: A systematic mapping study. In: IEEE. *2021 International Conference on Information Technology (ICIT)*. [S.l.], 2021. p. 719–724. Citado na página 16.

BENET, J. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014. Citado na página 40.

BERTINO, E.; TAKAHASHI, K. *Identity management: Concepts, technologies, and systems*. [S.l.]: Artech House, 2010. Citado na página 20.

BORGIA, E. The internet of things vision: Key features, applications and open issues. *Computer Communications*, Elsevier, v. 54, p. 1–31, 2014. Citado na página 15.

BOURAS, M. A. *et al.* A lightweight blockchain-based iot identity management approach. *Future Internet*, MDPI, v. 13, n. 2, p. 24, 2021. Citado 5 vezes nas páginas 34, 35, 42, 61 e 62.

CARDOSO, A. L. *et al.* Gerenciamento descentralizado de identidades para cidades inteligentes baseado na tecnologia blockchain. In: *Anais do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. Porto Alegre, RS, Brasil: SBC, 2022. p. 57–70. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/sbseg/article/view/21658>. Citado na página 76.

CHEN, J.; LIU, Y.; CHAI, Y. An identity management framework for internet of things. In: *2015 IEEE 12th International Conference on e-Business Engineering*. [S.l.: s.n.], 2015. p. 360–364. Citado 7 vezes nas páginas 37, 38, 42, 43, 44, 61 e 62.

Conceição, A. F. da; Rocha, V. E. M. *Blockchain: conceitos básicos*. [S.l.]: Amazon Kindle, 2020. ISBN 9798636424116. Citado 3 vezes nas páginas 23, 24 e 25.

DUNPHY, P.; PETITCOLAS, F. A. A first look at identity management schemes on the blockchain. *IEEE security & privacy*, IEEE, v. 16, n. 4, p. 20–29, 2018. Citado na página 31.

ESPOSTE, A. M. D. *et al.* Interscity: A scalable microservice-based open source platform for smart cities. In: SCITEPRESS. *International Conference on Smart Cities and Green ICT Systems*. [S.l.], 2017. v. 2, p. 35–46. Citado 2 vezes nas páginas 54 e 56.

FABIOLA, J. Blockchain e contratos inteligentes para aplicaÇÕes em iot, uma abordagem prÁtica. v. 2021, 2021. Citado 2 vezes nas páginas 26 e 28.

GHAFFARI, F. *et al.* Identity and access management using distributed ledger technology: A survey. *International Journal of Network Management*, Wiley Online Library, v. 32, n. 2, p. e2180, 2022. Citado na página 31.

HADDOUTI, S. E.; KETTANI, M. D. E.-C. E. Analysis of identity management systems using blockchain technology. In: IEEE. *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*. [S.l.], 2019. p. 1–7. Citado 2 vezes nas páginas 20 e 23.

HEWA, T.; YLIANTTILA, M.; LIYANAGE, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, Elsevier, v. 177, p. 102857, 2021. Citado na página 29.

ITU, I. T. U. *NGN identity management framework*. Itu-t y2720. International Telecomunication Union, 2009. Disponível em: <https://www.itu.int/rec/T-REC-Y.2720-200901-I>. Citado na página 20.

JONES, M. *JSON web key (JWK)*. [S.l.], 2015. Citado na página 48.

KHAN, M. A.; SALAH, K. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, Elsevier, v. 82, p. 395–411, 2018. Citado 2 vezes nas páginas 23 e 24.

KORTUEM, G. *et al.* Smart objects as building blocks for the internet of things. *IEEE Internet Computing*, IEEE, v. 14, n. 1, p. 44–51, 2009. Citado na página 15.

LIU, Y. *et al.* Blockchain-based identity management systems: A review. *Journal of network and computer applications*, Elsevier, v. 166, p. 102731, 2020. Citado 3 vezes nas páginas 20, 21 e 22.

MACEDO. Consenso distribuído eficiente no modelo síncrono particionado. v. 1, 2011. Citado na página 26.

MANOHAR, A.; BRIGGS, J. Identity management in the age of blockchain 3.0. *Workshop HCI for Blockchain*, Association for Computing Machinery, 2018. Citado na página 20.

MEKTOUBI, A. *et al.* New approach for securing communication over mqtt protocol a comparaison between rsa and elliptic curve. In: IEEE. *2016 Third International Conference on Systems of Collaboration (SysCo)*. [S.l.], 2016. p. 1–6. Citado na página 48.

MINGXIAO, D. *et al.* A review on consensus algorithm of blockchain. In: *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. [S.l.: s.n.], 2017. p. 2567–2572. Citado na página 29.

MÜHLE, A. *et al.* A survey on essential components of a self-sovereign identity. *Computer Science Review*, Elsevier, v. 30, p. 80–86, 2018. Citado 2 vezes nas páginas 20 e 23.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. 2008. Citado na página 23.

NEIROTTI, P. *et al.* Current trends in smart city initiatives: Some stylised facts. *Cities*, Elsevier, v. 38, p. 25–36, 2014. Citado na página 15.

OMAR, A. S.; BASIR, O. Identity management in iot networks using blockchain and smart contracts. 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)*. [S.l.: s.n.], 2018. p. 994–1000. Citado 6 vezes nas páginas 36, 42, 43, 44, 61 e 63.

QUEIROZ, F. G. G. e Leobino Sampaio Sampaio e Jauberth Abijaude Abijaude e Antonio Coutinho Coutinho e Ítalo Valcy Valcy e S. Q. Blockchain e a revolução do consenso sob demanda. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) - Minicursos*, 2018. Disponível em: <http://143.54.25.88/index.php/sbrcminicursos/article/view/1770>. Citado na página 29.

RAJASEKARAN, A. S.; AZEES, M.; AL-TURJMAN, F. A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, Elsevier, v. 52, p. 102039, 2022. Citado na página 31.

REBELLO, G. A. F. *et al.* Correntes de blocos: Algoritmos de consenso e implementação na plataforma hyperledger fabric. *Jornada de Atualização em Informática*, v. 2019, p. 93–148, 2019. Citado 2 vezes nas páginas 25 e 26.

SINGHAI, K. e. Distributed computing: Principles, algorithms, and systems. v. 1, 2008. Citado na página 25.

SZABO, N. Formalizing and securing relationships on public networks. *First monday*, 1997. Citado na página 29.

VENKATRAMAN, S.; PARVIN, S. *Developing an IoT Identity Management System Using Blockchain. Systems 2022, 10, 39*. [S.l.]: s Note: MDPI stays neutral with regard to jurisdictional claims in published . . . , 2022. Citado 7 vezes nas páginas 38, 42, 43, 44, 61, 62 e 63.

WANG, S. *et al.* DAG blockchain-based lightweight authentication and authorization scheme for IoT devices. *Journal of Information Security and Applications*, Elsevier, v. 66, p. 103134, 2022. Citado 6 vezes nas páginas 40, 41, 42, 43, 61 e 62.

XIE, J. *et al.* A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, IEEE, v. 21, n. 3, p. 2794–2830, 2019. Citado 2 vezes nas páginas 15 e 23.

ZHANG, K. *et al.* Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, IEEE, v. 55, n. 1, p. 122–129, 2017. Citado na página 16.

ZHU, X.; BADR, Y. Identity management systems for the internet of things: a survey towards blockchain solutions. *Sensors*, MDPI, v. 18, n. 12, p. 4215, 2018. Citado na página 21.

ZOU, W. *et al.* Smart contract development: Challenges and opportunities. *IEEE Transactions on Software Engineering*, v. 47, n. 10, p. 2084–2106, 2021. Citado na página 29.