Arquitetura de Software para Identidades Digitais Descentralizadas em Cidades Inteligentes: Um Relato de Experiência com a Trustchain

Marcelo P. Chequin[1], Carla O. Castanho[1 2], Fernando M. Neto[1], Paulo C. Vargas[1]

[1]Universidade Regional Integrada do Alto Uruguai e das Missões
Santiago – RS – Brazil

[2]Universidade Regional do Noroeste do Rio Grande do Sul
Ijui – RS – Brazil

{102513, carla.castanho, 066918, 102231}@urisantiago.br

carla.castanho@sou.unijui.edu.br

Abstract. *This article provides an overview of the relevance of decentralized architectures in the context of smart cities, highlighting the role of Decentralized Identifiers (DIDs) and describing the practical experience of installing the Trustchain system. The objective is to demonstrate the challenges, requirements, and benefits of this type of infrastructure.*

Resumo. *Este artigo apresenta uma visão geral da relevância das arquiteturas descentralizadas no contexto de cidades inteligentes, destacando o papel dos Identificadores Descentralizados (DIDs) e descrevendo a experiência prática da instalação do sistema de identificação descentralizado Trustchain. O objetivo é demonstrar os desafios, requisitos e benefícios desse tipo de infraestrutura.*

1. Introdução

A crescente digitalização de serviços públicos e privados, impulsionada pelas Tecnologias da Informação e Comunicação (TICs), ampliou a demanda por mecanismos confiáveis de identificação em ecossistemas conectados, incluindo as cidades inteligentes, onde múltiplos atores e dispositivos interagem continuamente. Nesse contexto, a identidade digital evoluiu de cadastros isolados para um elemento integrado aos serviços, exigindo autenticação, autorização e identificação consistentes, ao mesmo tempo que a proliferação de contas e credenciais e a dependência de provedores centralizados de autenticação evidenciaram limitações operacionais e de governança. Assim, compreender opções de infraestrutura para Identificadores Descentralizados (DIDs) torna-se relevante não só para determinar sua adoção, mas também para avaliar a viabilidade técnica diante dos desafios de integração, privacidade e interoperabilidade característicos de ambientes urbanos inteligentes [Ahad et al. 2020].

Do ponto de vista conceitual, a identidade digital pode ser entendida como um conjunto de atributos que habilita processos de autenticação, autorização e identificação em ambientes digitais [Rieger et al. 2021]. Modelos centralizados, amplamente difundidos, concentram dados e controles em poucos intermediários, o que levanta preocupações de privacidade, segurança e portabilidade. Por outro lado, abordagens descentralizadas

buscam uma adaptação mais interoperável e centrada no usuário. As especificações do W3C para DIDs e Credenciais Verificáveis (VCs) oferecem um arcabouço técnico para o modelo descentralizado, mesmo que sua implementação prática envolva decisões arquiteturais e tecnológicas que merecem investigação empírica.

Neste trabalho, apresenta-se um relato de experiência com a instalação, configuração e testes iniciais do sistema de identificação descentralizado Trustchain, uma infraestrutura de chave pública (DPKI), desenvolvida em Rust, que oferece suporte à criação, resolução e revogação de DIDs. A proposta é explorar a viabilidade técnica da solução, avaliando os requisitos necessários para sua operação e as dificuldades enfrentadas durante o processo de implementação. Embora a aplicação de DIDs em cidades inteligentes seja um tema emergente e relevante, este artigo não tem por objetivo defender sua adoção direta nesse contexto, mas sim descrever e analisar criticamente a experiência de trabalho com uma alternativa real de infraestrutura para identidades descentralizadas [Hobson et al. 2023]. O artigo está estruturado da seguinte forma para uma melhor compreensão do tema: a Seção 2 apresenta os principais conceitos sobre identidade digital e as diferenças entre os modelos centralizado e descentralizado para identidade digital; a Seção 3 demonstra a parte técnica sobre o sistema de identificação digital descentralizado Trustchain e a Seção 4 apresenta as conclusões e os principais pontos para trabalhos futuros.

2. Referencial Teórico

Esta seção apresenta os fundamentos conceituais que sustentam o estudo. Inicialmente, discute-se o conceito de identidade digital no contexto da crescente conectividade e da multiplicação de contas e credenciais. Em seguida, contrastam-se as arquiteturas centralizada e descentralizada, destacando implicações de privacidade, segurança e governança. Por fim, introduzem-se os padrões do W3C para Identificadores Descentralizados (DIDs) e Credenciais Verificáveis (VCs), que servirão de base para a análise técnica desenvolvida nas seções subsequentes.

2.1. Identidade Digital

Nas últimas décadas, a sociedade passou por profundas transformações em seus modos de interação, impulsionadas pela crescente conectividade digital. Praticamente todos os setores migraram suas operações para plataformas online — desde bancos e e-commerces até sistemas de comunicação e serviços de mobilidade urbana. Esse novo cenário digital exige que as organizações reformulem suas estratégias de atuação, revendo suas formas de comunicação, comercialização e relacionamento com diferentes agentes do ecossistema. Para os usuários, essa transição alterou significativamente os hábitos de consumo e interação, tornando comuns as transações virtuais e, com isso, reduzindo ou até substituindo os meios tradicionais de estabelecimento de confiança. [Dib and Toumi 2020]

Nesse contexto, o uso intensivo de serviços digitais passou a exigir a criação de múltiplas contas e credenciais em diferentes plataformas, fazendo com que os cidadãos se tornassem cada vez mais dependentes de sistemas de autenticação centralizados. Empresas como Google e Facebook passaram a oferecer mecanismos de login único, concentrando o controle das identidades digitais dos usuários. A identidade digital, nesse cenário, é entendida como um conjunto de atributos associados a uma pessoa

ou organização, que viabiliza processos de autenticação, autorização e identificação em ambientes digitais. Esses atributos — como documentos, nacionalidade e endereços — podem ser atualizados, revogados ou transferidos, permitindo a validação da identidade em diferentes contextos online. [Goodell and Aste 2019]

No campo das identidades digitais, dois modelos principais têm sido discutidos: o modelo centralizado e o descentralizado. Em cidades inteligentes, a estrutura ainda é majoritariamente centralizada, com dados concentrados em silos controlados por plataformas específicas. Essa centralização, embora funcional, levanta preocupações sérias quanto à privacidade, segurança da informação e tratamento ético dos dados pessoais. Como alternativa, surge o modelo descentralizado de identidade digital, que visa contornar essas fragilidades, oferecendo uma abordagem centrada no usuário, mais transparente e com maior controle sobre os próprios dados. [Goodell and Aste 2019]

2.2. Identidade Digital Centralizada

O modelo tradicional de identidade digital é amplamente utilizado na atualidade e baseia-se na relação entre o usuário e uma organização que administra o sistema de identificação. Nesse formato, a instituição — seja ela uma empresa privada, banco, rede social, serviço de e-commerce ou órgão governamental — atua como autoridade central, sendo responsável por coletar, armazenar e gerenciar os dados pessoais do usuário, como nome, e-mail, documentos e informações de navegação. Essa centralização torna a organização controladora da identidade, oferecendo acesso aos serviços mediante autenticação dos dados por ela mantidos. [Rieger et al. 2021]

Tal abordagem está tão enraizada nas rotinas digitais que, atualmente, a autenticação por login e senha tornou-se a principal forma de acesso a plataformas online. Embora tenha sido essencial para viabilizar a digitalização de serviços e permitir a representação virtual de pessoas e instituições, esse modelo traz consigo limitações relevantes. A dependência de uma única autoridade central para validação da identidade gera fragmentação — já que o usuário precisa criar múltiplas contas para diferentes serviços — e reduz a eficiência, ao passo que os dados ficam restritos aos servidores de cada plataforma. Essa fragmentação também intensifica os riscos de segurança e privacidade, uma vez que falhas ou vazamentos afetam diretamente os dados sensíveis dos usuários. [Rieger et al. 2021]

Além disso, a forma como os dados são tratados em sistemas centralizados varia conforme as diretrizes e regulamentações adotadas por cada provedor. Em setores regulados, como bancos ou instituições públicas, há exigência de processos de verificação mais rígidos. Por outro lado, em ambientes menos controlados, como redes sociais, é possível criar múltiplas identidades — inclusive falsas — sem barreiras significativas. Essa flexibilidade, aliada à concentração de dados em poucas entidades, tem motivado uma série de estudos que investigam formas de reduzir os riscos desse modelo. Como resposta, emergem as identidades digitais descentralizadas, que propõem uma nova arquitetura: mais segura, transparente e com foco na autonomia do usuário, reduzindo a necessidade de intermediários e permitindo maior controle sobre os próprios dados.

2.3. Identidade Digital Descentralizada

No contexto das arquiteturas descentralizadas, cada entidade pode ser representada por um Identificador Descentralizado (Decentralized Identifier – DID), um padrão proposto

pelo W3C. Os DIDs são identificadores únicos, globais e persistentes, que permitem a autenticação de entidades sem a necessidade de intermediários confiáveis ou bases de dados centralizadas. Um DID é vinculado a um documento DID (DID Document), que armazena informações como chaves públicas e métodos de verificação, possibilitando a realização de interações seguras, criptografadas e auditáveis. Com isso, as entidades passam a ter controle direto sobre sua identidade digital, podendo comprovar atributos de forma seletiva e com maior privacidade.[W3C Credentials Community Group 2022]

Essa abordagem é especialmente relevante em contextos que exigem confiança e interoperabilidade, como aplicações em cidades inteligentes, saúde digital, educação e Internet das Coisas (IoT). Ao eliminar o ponto único de controle típico das arquiteturas centralizadas, os DIDs fortalecem a segurança, reduzem o risco de vazamento de dados e aumentam a autonomia dos usuários sobre suas informações pessoais. Além disso, a compatibilidade com credenciais verificáveis permite que entidades compartilhem apenas os dados necessários, respeitando princípios de minimização e consentimento, o que reforça a ética no tratamento de dados digitais.

2.4. Identificadores Descentralizados (DIDs) e Credenciais Verificáveis (VCs)

Os Identificadores Descentralizados (DIDs) são URIs padronizados que identificam, de forma global e persistente, pessoas, organizações ou dispositivos sem depender de autoridades centrais. Um DID tem a forma `did:<método>:<id>`, é resolvido para um *DID document* (com chaves públicas, relações de verificação e *service endpoints*) e pode ser estendido por uma *DID URL* para referenciar recursos específicos dentro do documento. A criação, atualização e desativação de DIDs é definida por *DID methods*, que operam sobre um *verifiable data registry* (ledger, rede P2P, IPFS), permitindo práticas essenciais como rotação de chaves e recuperação de controle [W3C Credentials Community Group 2022].

As Credenciais Verificáveis (VCs) modelam afirmações assinadas sobre um sujeito (atributos, qualificações, status) dentro do triângulo emissor–titular–verificador. O ciclo de emissão, apresentação e verificação é baseado em provas criptográficas e pode incluir estado/revogação e divulgação seletiva, de modo que apenas os dados necessários ao propósito sejam revelados. Na prática, isso permite validar um diploma, uma habilitação ou o status de um dispositivo IoT sem expor informações excedentes e com menor risco de correlação, por exemplo, usando DIDs pareados [W3C Credentials Community Group 2022]. Para uma melhor compreensão do tema, a Figura 1 apresenta uma visão geral da arquitetura baseada em DIDs, destacando os principais componentes e seus papéis no ecossistema de identidades descentralizadas.

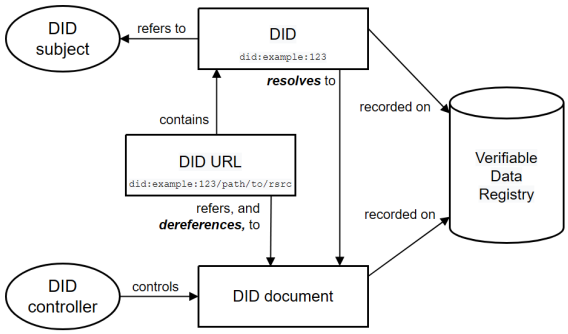

Figura 1. Visão geral da arquitetura DID e do relacionamento dos componentes básicos.

Fonte: [W3C Credentials Community Group 2022]

Os termos apresentados na Figura 1 demonstram os componentes centrais da arquitetura baseada em DIDs. O *DID subject* é a entidade a que o DID se refere (por exemplo, a egressa Ana Silva ou um semáforo IoT). O *DID* (`did:example:123`) é o identificador que resolve para o *DID document*, onde estão as chaves e as relações de verificação; esse documento é registrado em um *verifiable data registry* para garantir auditabilidade e integridade. O *DID controller* (quem controla chaves e atualizações) pode ser o próprio sujeito — por exemplo, Ana, via sua carteira — ou, no caso do semáforo, a Secretaria de Mobilidade. A *DID URL* (ex.: `did:example:123#key-1`) referencia uma chave específica no documento, permitindo que um verificador obtenha exatamente o material criptográfico necessário para validar uma apresentação verificável. Concretamente, ao checar o diploma de Ana, o serviço municipal resolve o DID dela no registro, dereferencia `#key-1` para obter a chave correta e valida a assinatura da credencial; se a universidade rotacionou chaves, a verificação permanece consistente porque o documento atualizado é recuperado na resolução. Em IoT, o controlador de tráfego aplica o mesmo fluxo para aceitar um alerta autenticado do semáforo antes de acionar uma intervenção.

3. Sistema de Identificação Digital Descentralizado Trustchain

Com o surgimento de diferentes propostas voltadas ao desenvolvimento de soluções para identidade digital descentralizada, a busca por uma infraestrutura interoperável, segura e centrada no usuário tem se intensificado. Nesse cenário, destaca-se o sistema *Trustchain*, uma iniciativa que oferece uma abordagem robusta para enfrentar os desafios associados à gestão de identidades digitais. Enquanto os sistemas centralizados de identificação digital concentram os processos de registro e administração de identificadores exclusivos em bancos de dados centralizados — o que implica em riscos à privacidade, vulnerabilidades de segurança e dependência de intermediários —, os sistemas descentralizados surgem como uma alternativa mais resiliente, distribuída e orientada à privacidade. Contudo, muitas dessas soluções ainda dependem de infraestruturas pré-existentes ou de entidades centralizadas em alguma etapa da cadeia de confiança, o que limita sua autonomia plena [Hobson et al. 2023].

3.1. Apresentação Técnica Trustchain

Trustchain é uma implementação livre e de código aberto de uma Infraestrutura de Chave Pública Descentralizada (DPKI) orientada aos padrões do W3C para

DIDs e VCs, projetada para prover endereçabilidade, verificabilidade e auditabilidade de identidades digitais sem pontos únicos de confiança [Hobson et al. 2023, W3C Credentials Community Group 2022]. O núcleo é desenvolvido em **Rust**, explorando segurança de memória e alto desempenho para operações criptográficas e validações de estado; a publicação e resolução de DIDs é realizada via **ION** (método DID ancorado em **Bitcoin**), enquanto o conteúdo dos *DID documents* e metadados associados é distribuído em **IPFS**. Essa composição separa imutabilidade/ordenação temporal (Bitcoin/ION) do armazenamento de conteúdo (IPFS), reduzindo acoplamento e custo operacional.

3.2. Arquitetura Trustchain

A figura 2 apresenta a arquitetura funcional da Trustchain, evidenciando suas camadas e principais dependências externas. O objetivo é mostrar como o servidor expõe serviços para clientes, como o núcleo em Rust orquestra o ciclo de vida dos DIDs, e de que forma a integração com ION/Bitcoin e IPFS fornece, respectivamente, ancoragem imutável e distribuição de documentos. Essa visão geral facilita compreender, nos parágrafos subsequentes, o papel de cada componente e o fluxo de criação, resolução e revogação de identidades.

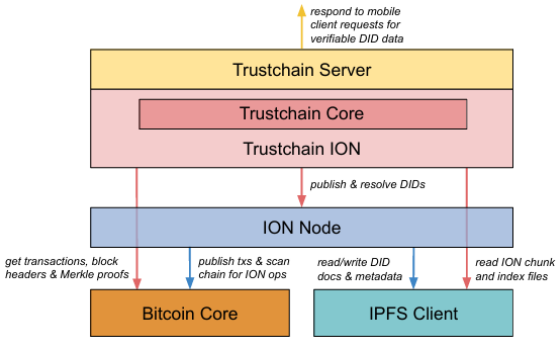

Figura 2. ***Arquitetura funcional da Trustchain integrada à ION/Bitcoin e IPFS.***
Fonte: [Hobson et al. 2023]

Conforme a Figura 2, a arquitetura é modular e em camadas. No topo, o **Trustchain Server** expõe interfaces (REST/gRPC) para carteiras e serviços, atendendo a requisições por dados verificáveis e orquestrando o ciclo de vida das identidades. O **Trustchain Core**, escrito em **Rust**, centraliza a lógica de identidade: geração e rotação de chaves, montagem e validação de cadeias de confiança (DIDs-raiz $\rightarrow$ *downstream* DIDs), validação de *timestamping* e aplicação de políticas de revogação/estado. O módulo **Trustchain ION** atua como adaptador para a rede **ION**, traduzindo operações locais para os tipos *create*, *update* e *deactivate*. Na camada intermediária, o **ION Node** publica operações ancoradas no **Bitcoin** (via **Bitcoin Core**) e indexa o estado efetivo dos DIDs; em paralelo, realiza leitura e escrita de documentos e metadados em **IPFS**. Em apoio ao ambiente, **Node.js** pode prover utilitários/serviços auxiliares, **MongoDB** persistir metadados operacionais (filas, estados, logs) e **Git** versionar código e *infra-as-code*. Essa composição assegura que a imutabilidade e a ordem temporal provenham da cadeia do Bitcoin/ION, enquanto o conteúdo (documentos DID, listas de status) seja distribuído

pelo IPFS, mantendo custos baixos, disponibilidade elevada e interoperabilidade com o ecossistema W3C.

3.3. Fluxos Operacionais da Trustchain

Na prática, o *fluxo de criação* (*create*) inicia-se no *Core*, que gera um par de chaves e o *DID document* inicial (métodos de verificação, relações e *service endpoints*); o documento é então persistido em IPFS, produzindo um *Content Identifier* (CID). Em seguida, o adaptador ION compõe a operação de criação referenciando esse CID e a ancora no Bitcoin via *ION Node*, o que confere registro imutável e *timestamp* verificável; o sistema retorna o `did:<método>:<id>` e metadados de prova para auditoria. O *fluxo de resolução* (*resolve*) toma um `did:<método>:<id>` — ou uma `DID URL` com fragmento, como `#key-1` — e, a partir do *ION Node*, recupera o estado atual do DID considerando todas as operações válidas; o documento correspondente é obtido do IPFS (com verificação de integridade pelo CID), enquanto o *Core* valida a cadeia de confiança (DID-raiz $\rightarrow$ dDID), as assinaturas e o *timestamping*, e dereferencia o recurso apontado (por exemplo, a chave pública do fragmento `#key-1`) para uso na verificação de VCs/VPs. Já os *fluxos de atualização e revogação* (*update/deactivate*) são iniciados pelo *controller* do DID, que assina a operação para rotacionar chaves, alterar *endpoints* ou desativar o identificador; a operação é publicada e ancorada via ION/Bitcoin, e os resolutores passam a refletir o novo estado. A Trustchain acrescenta mecanismos de **completude de revogação**, garantindo que listas/estruturas de estado sejam auditáveis e não-omitíveis, mitigando janelas nas quais credenciais revogadas pudessem parecer válidas.

Alguns recursos técnicos merecem destaque. A combinação **DPKI + *timestamping*** verificável em Bitcoin minimiza a confiança depositada na infraestrutura subjacente, deslocando a raiz de verificabilidade para provas objetivas de inclusão em bloco. O encadeamento entre **DIDs-raiz e dDIDs** permite espelhar hierarquias institucionais e endereçar o "*oracle problem*" ao estabelecer, de forma auditável, as âncoras de confiança aceitas por uma comunidade. Existe a privacidade por construção, compatível com VCs/VPs e *selective disclosure*, com incentivo ao uso de DIDs pareados para reduzir correlação entre domínios. No campo operacional, há suporte a rotação de chaves, recuperação de controle e controles multi-parte conforme a política do controlador. Por fim, a aderência ao *DID Core* e ao *VC Data Model* assegura interoperabilidade e o desacoplamento entre resolução (ION/Bitcoin/IPFS) e verificação de credenciais no nível aplicativo.

No uso cotidiano para a validação de um diploma, a carteira do usuário solicita ao *Trustchain Server* os dados verificáveis do emissor e do titular; o *Core* resolve os DIDs na ION, recupera os documentos do IPFS, valida *timestamps* e cadeias e aplica políticas de estado/revogação. Para apresentação, gera-se uma *Verifiable Presentation* com divulgação seletiva; o verificador obtém as chaves referenciadas via (`DID URL`) e valida a assinatura da VC. Em cenários de IoT, o mesmo fluxo é aplicado a dispositivos: um controlador de tráfego somente aceita eventos autenticados após resolver o DID do dispositivo e validar o material criptográfico indicado pelo fragmento de chave, garantindo autenticidade e redução de superfícies de ataque.

3.4. Preparação do Ambiente e Implantação do Protótipo

A implementação foi conduzida em uma máquina virtual Linux (Debian 12). Em linhas gerais, o processo divide-se em três etapas: (i) preparar o ambiente da **ION** (Identity Overlay Network), (ii) instalar a linguagem **Rust**, e (iii) compilar e configurar a **Trustchain**. A ION — método DID de código aberto — ancora operações na *blockchain* do **Bitcoin** e armazena documentos no **IPFS**, exigindo como pré-requisitos **Node.js** (e seu gerenciador de pacotes), **MongoDB**, **Bitcoin Core** e o próprio **IPFS**. Optou-se pela *testnet* do Bitcoin para desenvolvimento; a sincronização inicial do *Bitcoin Core* demandou alguns dias, pois foi necessário baixar e validar toda a cadeia de blocos. Concluída essa etapa, a ION foi ajustada por meio de variáveis de ambiente e arquivos de configuração, garantindo que *IPFS*, *MongoDB* e *Bitcoin Core* estivessem ativos e estáveis. Em seguida, instalou-se o **Rust** (via `rustup`) e procedeu-se à compilação e configuração da **Trustchain**, definindo diretórios de dados e parâmetros operacionais. Ao final, o ambiente passou a permitir a criação e publicação de DIDs com ancoragem e *timestamp* verificáveis [Castanho et al. 2025].

Para os testes, foi necessário provisionar fundos na carteira em *testnet* — já que a criação de novos DIDs referencia o CID do documento no **IPFS** dentro de uma transação do **Bitcoin**. Instanciou-se o servidor HTTP da Trustchain, utilizado como emissor e verificador de credenciais via API. Nessa configuração, gerou-se o DID do emissor (utilizado como argumento de inicialização), definiu-se o *FQDN* do servidor (endpoint consumido pelo aplicativo móvel), registrou-se o carimbo de data/hora do DID raiz e habilitou-se **TLS** na porta 443 (certificado *Let's Encrypt* emitido via *Certbot*). Com o serviço em execução, um DID representando uma "carteira de motorista" foi emitido pela interface web do servidor, que também disponibiliza o QR Code correspondente. As mensagens de log confirmam cada requisição atendida. No *Trustchain Mobile*, configurou-se o *endpoint* do servidor e a data do evento raiz; a leitura do QR pelo aplicativo permite ao usuário importar o DID/credencial e, a partir daí, realizar apresentações verificáveis com divulgação seletiva em cenários de validação (por exemplo, comprovação de atributos a terceiros) [Castanho et al. 2025].

4. Conclusão e Trabalhos Futuros

Este artigo abordou o problema da gestão de identidades digitais em contextos de cidades inteligentes e explorou a *Trustchain* como opção de infraestrutura para Identificadores Descentralizados (DIDs). Adotou-se uma metodologia de relato de experiência, documentando a instalação, configuração e testes iniciais de um protótipo em ambiente controlado (VM Debian 12) que integra ION/Bitcoin (testnet), IPFS, MongoDB e o núcleo em Rust. Foram exercitados os fluxos de criação, resolução, atualização e revogação de DIDs, além de um cenário de validação de credencial (emissão e apresentação via QR Code e aplicativo móvel), com ancoragem e rastreabilidade temporal verificáveis.

Os resultados apontam que a Trustchain é tecnicamente viável para prototipagem de DIDs alinhados ao *DID Core* e ao *VC Data Model* do W3C, oferecendo auditabilidade (provas em Bitcoin), desacoplamento de conteúdo (IPFS), privacidade por construção e boa base de segurança/performace pelo uso de Rust. Em contrapartida, observou-se complexidade operacional relevante: sincronização inicial demorada do *Bitcoin Core*, necessidade de coordenação entre múltiplos serviços (ION, IPFS, MongoDB, servidor

HTTP), provisão de fundos em *testnet*, dependência de conectividade estável e latências associadas à confirmação de transações. Do ponto de vista prático, a solução se mostra adequada para laboratóriose pilotos, enquanto uma adoção em escala municipal demandará mecanismos de governança, observabilidade (logs, métricas e alertas), automação de implantação e aprimoramentos de usabilidade para carteiras e operadores.

Como trabalhos futuros, pretende-se integrar o protótipo a serviços urbanos reais — como credenciais acadêmicas, passes de mobilidade e identidades de dispositivos IoT — e avaliar desempenho e latência sob carga; em paralelo, avançar no monitoramento e trilhas de auditoria e por fim, comparar sistematicamente a Trustchain com outros métodos DID e arranjos de identidade autossoberana, mapeando custos, riscos e aderência regulatória em cenários de cidades inteligentes.

Agradecimentos

Esta pesquisa foi parcialmente financiada pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), por meio dos projetos 309425/2023-9, 402915/2023-2. Agradecimentos especiais ao Dr. Rafael Z. Frantz pela revisão de uma versão preliminar deste artigo.

Referências

[Ahad et al. 2020] Ahad, M., Paiva, S., Tripathi, G., and Feroz, N. (2020). Enabling technologies and sustainable smart cities. *Sustainable Cities and Society*, 61:102301.

[Castanho et al. 2025] Castanho, C., Frantz, R., Chequin, M., Sawicki, S., Roos-Frantz, F., Molina-Jimenez, C., Crowcroft, J., and Hobson, T. (2025). Unlocking the potential of decentralised digital identification systems for smart cities. In *Anais do III Colóquio em Blockchain e Web Descentralizada*, pages 7–12, Porto Alegre, RS, Brasil. SBC.

[Dib and Toumi 2020] Dib, O. and Toumi, K. (2020). Decentralized identity systems: Architecture, challenges, solutions and future directions. *Annals of Emerging Technologies in Computing*, 4:19–40.

[Goodell and Aste 2019] Goodell, G. and Aste, T. (2019). A decentralised digital identity architecture.

[Hobson et al. 2023] Hobson, T., France, L., Greenbury, S., Hare, L., and Wochner, P. (2023). Trustchain – trustworthy decentralised public key infrastructure for digital credentials. volume 2023.

[Rieger et al. 2021] Rieger, A., Fridgen, G., Sedlmeir, J., and Smethurst, R. (2021). Digital identities and verifiable credentials. *Business Information Systems Engineering*, 63.

[W3C Credentials Community Group 2022] W3C Credentials Community Group (2022). Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. `https://www.w3.org/TR/did-1.0/`. Accessed: 2025-08-13.