Universidade Estadual de Londrina

PEDRO EDUARDO GARBOSSA DE ALMEIDA

IDENTIDADE AUTO SOBERANA: DESAFIOS E OPORTUNIDADES NA PRESTAÇÃO DE SERVIÇOS PÚBLICOS

LONDRINA
2024

PEDRO EDUARDO GARBOSSA DE ALMEIDA

IDENTIDADE AUTO SOBERANA: DESAFIOS E OPORTUNIDADES NA PRESTAÇÃO DE SERVIÇOS PÚBLICOS

Versão Preliminar de Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Bruno Bogaz Zarpelão

LONDRINA

2024

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

Sobrenome, Nome.
Título do Trabalho : Subtitulo do Trabalho / Nome Sobrenome. - Londrina, 2017.
100 f. : il.

Orientador: Nome do Orientador Sobrenome do Orientador.
Coorientador: Nome Coorientador Sobrenome Coorientador.
Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Ciência da Computação, 2017.
Inclui bibliografia.

1. Assunto 1 - Tese. 2. Assunto 2 - Tese. 3. Assunto 3 - Tese. 4. Assunto 4 - Tese. I. Sobrenome do Orientador, Nome do Orientador. II. Sobrenome Coorientador, Nome Coorientador. III. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação. IV. Título.

PEDRO EDUARDO GARBOSSA DE ALMEIDA

IDENTIDADE AUTO SOBERANA: DESAFIOS E OPORTUNIDADES NA PRESTAÇÃO DE SERVIÇOS PÚBLICOS

Versão Preliminar de Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação.

BANCA EXAMINADORA

Orientador: Prof. Dr. Bruno Bogaz Zarpelão
Universidade Estadual de Londrina

Prof. Dr. Segundo Membro da Banca
Universidade/Instituição do Segundo Membro da Banca – Sigla instituição

---

Prof. Dr. Terceiro Membro da Banca
Universidade/Instituição do Terceiro Membro da Banca – Sigla instituição

Londrina, 24 de novembro de 2024.

AGRADECIMENTOS

Os agradecimentos principais são direcionados à Gerald Weber, Miguel Frasson, Leslie H. Watter, Bruno Parente Lima, Flávio de Vasconcellos Corrêa, Otavio Real Salvador, Renato Machnievscz[1] e todos aqueles que contribuíram para que a produção de trabalhos acadêmicos conforme as normas ABNT com LaTeX fosse possível.

Agradecimentos especiais são direcionados ao Centro de Pesquisa em Arquitetura da Informação[2] da Universidade de Brasília (CPAI), ao grupo de usuários *latex-br*[3] e aos novos voluntários do grupo *abnTeX2*[4] que contribuíram e que ainda contribuirão para a evolução do abnTeX2.

[1] Os nomes dos integrantes do primeiro projeto abnTeX foram extraídos de <http://codigolivre.org.br/projects/abntex/>

[2] <http://www.cpai.unb.br/>

[3] <http://groups.google.com/group/latex-br>

[4] <http://groups.google.com/group/abntex2> e <http://abntex2.googlecode.com/>

"Não vos amoldeis às estruturas deste mundo, mas transformai-vos pela renovação da mente, a fim de distinguir qual é a vontade de Deus: o que é bom, o que Lhe é agradável, o que é perfeito.
(Bíblia Sagrada, Romanos 12, 2))

ALMEIDA, P. E. G. DE. **Identidade Auto Soberana: Desafios e oportunidades na prestação de serviços públicos**. 2024. 28f. Trabalho de Conclusão de Curso – Versão Preliminar (Bacharelado em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2024.

RESUMO

Nas últimas décadas, a autenticação centralizada tem sido amplamente empregada em sistemas e plataformas, apresentando desafios significativos no gerenciamento de identidades, uma vez que os usuários frequentemente carecem de controle sobre seus próprios dados. Este fenômeno, associado ao crescente uso de diversas plataformas e sistemas, tem contribuído para o aumento substancial de incidentes de vazamento de dados, culminando em sérias questões relacionadas à privacidade. Em resposta a esse cenário, tem-se verificado um aumento nas discussões voltadas à aprimoração das práticas de gestão de identidades digitais. Nesse contexto, destaca-se o conceito de Identidade Auto-Soberana (SSI, do inglês *Self-Sovereign Identity*) como uma abordagem inovadora para a administração de identidades digitais. Este trabalho tem como objetivo propor um modelo que utiliza o conceito de SSI para facilitar a prestação de serviços públicos, além de identificar e discutir os desafios associados à implementação do SSI.

Palavras-chave: Identidade Auto Soberana. Privacidade. Identidade Digital.

ALMEIDA, P. E. G. DE. **Self-Sovereign Identity: Challenges and opportunities in providing public services**. 2024. 28p. Final Project – Draft Version (Bachelor of Science in Computer Science) – State University of Londrina, Londrina, 2024.

ABSTRACT

In recent decades, centralized authentication has been widely employed in systems and platforms, presenting significant challenges in identity management, since users often lack control over their own data. This phenomenon, coupled with the growing use of various platforms and systems, has contributed to a substantial increase in data leakage incidents, culminating in serious privacy issues. In response to this scenario, there has been an increase in discussions aimed at improving digital identity management practices. In this context, the concept of Self-Sovereign Identity (SSI) stands out as an innovative approach to managing digital identities. This work aims to propose a model that uses the SSI to facilitate the provision of public services, in addition to identifying and discussing the challenges associated with the implementation of SSI.

Keywords: Self-Sovereign Identity. Privacy. Digital Identity.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

SSI	Self-Sovereign Identity
VCs	Verifiable Credentials
DIDs	Decentralized Identifiers
VPs	Verifiable Presentations
URI	Uniform Resource Identifier
CPF	Cadastro de Pessoa Física
IIPR	Instituto de Identificação do Paraná
Detran	Departamento Estadual de Trânsito
CNH	Carteira Nacional de Habilitação
SUS	Sistema Único de Saúde
P2P	Peer-to-Peer
W3C	World Wide Web Consortium

SUMÁRIO

1 INTRODUÇÃO

A era digital trouxe consigo uma série de avanços e transformações na forma como lidamos com a identidade e os dados pessoais. No entanto, o paradigma atual de autenticação e gestão de identidade frequentemente se baseia em sistemas centralizados, nos quais os usuários cedem o controle de seus dados a terceiros [1].

Neste contexto, surge o conceito de Identidade Auto-Soberana (SSI, do inglês *Self-Sovereign Identity*), uma abordagem inovadora que visa proporcionar aos usuários o controle total sobre suas próprias identidades digitais. No âmbito do SSI, os usuários detêm o poder de gerenciar e compartilhar seus dados de forma segura e descentralizada, sem depender de autoridades centrais ou intermediárias [2]. Desse modo, tem-se um dos primeiros desafios na implementação do SSI: a curva de aprendizado. Isso se deve à transferência da responsabilidade pelo gerenciamento de chaves, do provedor centralizado para o usuário. Caso o usuário venha a perder essas chaves, isso resultará na perda irreversível de informações [1].

O presente trabalho propõe um modelo que utiliza o conceito de SSI para facilitar a prestação de serviços públicos, focando especificamente em serviços que oferecem benefícios e exigem credenciais para comprovar informações necessárias para obtenção desses benefícios. Por exemplo, para obter o benefício de estudante na instituição responsável pelo transporte público de uma cidade, o estudante deve fornecer um comprovante de matrícula. Para a concessão de auxílio de renda, é exigida a comprovação de renda e outras informações.

Nestes cenários, o modelo proposto atuaria como uma ponte entre as instituições, permitindo que o usuário mantenha o controle de suas credenciais e forneça apenas as informações necessárias para obter o benefício desejado. Assim, o usuário teria a responsabilidade e o poder de gerenciar suas próprias credenciais, garantindo uma maior segurança e privacidade dos dados pessoais.

Um dos desafios na adoção do SSI é estabelecer uma comunicação confiável entre as entidades responsáveis pela verificação e validação de credenciais digitais [1]. Por isso, serão investigadas tecnologias primordiais para o funcionamento eficiente do SSI, abrangendo a criptografia de dados, a tecnologia blockchain e o uso de identificadores descentralizados. A aplicação dessas ferramentas possibilitará o desenvolvimento de um sistema no qual os usuários poderão compartilhar apenas as informações necessárias para cada contexto específico, preservando sua privacidade e segurança.

2 FUNDAMENTAÇÃO TEÓRICO-METODOLÓGICA E ESTADO DA ARTE

2.1 Privacidade

Privacidade é a habilidade que um indivíduo possui de controlar quais informações de si ele deseja ou não expor. Assim, o indivíduo possui a seletividade de determinar quais informações de si poderão ser usadas por terceiros [3].

Atualmente ocorre um ofuscamento das fronteiras da privacidade, e estamos em direção ao amplo acesso à informação. Com isso surge a necessidade de restringir o acesso a alguns dados [4]. Ao utilizar uma mídia social, o usuário coloca nela suas informações, com isso, é montado uma espécie de "portfólio" da sua pessoa. Esse portfólio pode ser trocado ou vendido para outras empresas ou até mesmo para o governo [3].

Devido a tudo isso, discursos sobre direito à privacidade vem tomando o cotidiano, pois uma característica bem presente nos dias de hoje é a exposição. As informações pessoais são cada vez mais acessíveis, tornando essa exposição ainda maior com as redes sociais [3]. A seletividade em compartilhar informações de forma restrita no espaço pessoal acaba assumindo características diferentes neste ambiente digital. Neste cenário é proporcionado novas maneiras de expressão, mas ao mesmo tempo é aberto um caminho para novas formas de violação. Os dados que são compartilhados livremente na internet não podem mais ser totalmente recuperados para a esfera privada, pois o controle desses dados já não pode ser mais garantido [4]. Por isso torna-se necessário que o usuário volte a ter controle sobre seus dados.

2.2 Gerenciamento de identidade

Com o progresso da era digital, tornou-se indispensável a utilização de plataformas de comércio eletrônico[1], instituições bancárias[2] e demais serviços online. Em decorrência disso, observou-se uma ampla disseminação de dados, uma vez que, frequentemente, os usuários são requeridos a efetuar cadastros em cada site visitado [5]. Esses provedores de serviços utilizam mecanismos de autorização, os quais asseguram que apenas usuários autorizados terão acesso e poderão usufruir dos serviços oferecidos. Dessa forma, surgiu a necessidade do emprego de identidades digitais e de um método eficiente para seu gerenciamento [6].

Uma identidade digital é composta pela combinação de subconjuntos de informações, denominados identidades parciais. Alguns desses subconjuntos, como o Cadastro de

[1] <https://neilpatel.com/br/blog/e-commerce-no-brasil/>
[2] <https://senhorcontabil.com.br/blog/impactos-do-crescimento-do-numero-de-bancos-digitais/>

Pessoa Física (CPF), são capazes de identificar alguém de forma única. A representatividade de uma identidade parcial é contextual e varia de acordo com o ambiente em que está inserida. Por exemplo, em uma instituição educacional, a identidade parcial pode conter informações como número de matrícula, curso e data de nascimento. Em contrapartida, em um ambiente corporativo, essa identidade parcial pode incluir dados como endereço, número de identificação, funções e privilégios específicos de um funcionário [6].

Por sua vez, um sistema de gerenciamento de identidades proporciona ferramentas para administrar essas identidades parciais no ambiente digital. Esse sistema é dotado de funcionalidades que permitem a administração, descoberta e troca de informações, garantindo a identificação de uma entidade e suas informações associadas. Cabe ao sistema decidir quais informações serão compartilhadas com outra entidade. Atualmente, existem quatro modelos de sistemas de gerenciamento de identidades: Tradicional, Federado, Centralizado e Centrado no Usuário [6, 7].

- O modelo **Tradicional**: amplamente adotado por provedores de serviços, os provedores atuam como fornecedores e administradores de identidades digitais. Nesse formato, os usuários são solicitados a inserir suas informações, recebendo, em troca, uma identificação exclusiva para o provedor específico (como um login), neste modelo não há comunicação entre diferentes provedores [6]. Este modelo implica em custos significativos para os usuários e os expõe a um risco de segurança considerável [8]. Em caso de vazamento de dados, todas as informações fornecidas pelos usuários podem ser comprometidas, como ilustrado pelo incidente ocorrido em 2019, no qual o grupo hoteleiro internacional Marriott foi multado em quase £100 milhões. Investigações descobriram que hackers haviam roubado os registros de 339 milhões de hóspedes, evidenciando as vulnerabilidades desse modelo tradicional [9].

- O modelo **Federado**: surgiu como uma alternativa à inflexibilidade do modelo tradicional, fundamentando-se no compartilhamento de identidades digitais entre diversos provedores de serviços e na ideia de autenticação única. Exemplificando, destacam-se o Google Account[3] e o Microsoft Account[4], que disponibilizam apenas as informações necessárias para os diferentes provedores utilizados. Contudo, a desvantagem desse modelo reside no fato de que os usuários cederem o controle de seus dados a grandes corporações privadas [6, 8].

- O modelo **Centralizado**: a autenticação de usuários é gerenciada por uma única entidade central, que atua como o ponto de controle para o acesso a sistemas e serviços. Nesse modelo, todas as credenciais e informações de autenticação são mantidas e gerenciadas por esse ponto central, muitas vezes denominado como um servidor de

[3] <https://www.google.com/account/about/>
[4] <https://account.microsoft.com/account>

autenticação [10]. Dessa forma, nota-se que o risco desse modelo é que, se o servidor de autenticação falhar ou for comprometido, todo o sistema fica em risco [6].

- O modelo **Centrado no Usuário**: baseia-se na premissa de devolver ao usuário o controle de seus próprios dados. Este modelo surge como uma resposta à mercantilização da identidade digital por corporações privadas. Nele, o usuário armazena suas identidades digitais em uma espécie de carteira digital, sendo ele mesmo o responsável por liberar as informações solicitadas por um provedor de serviço [6, 8].

O modelo de gerenciamento de identidade que tem ganhado destaque nos tempos atuais é o modelo de identidades federadas. Essa abordagem otimiza a troca de informações relacionadas às identidades com base na confiança estabelecida entre as diferentes federações. É amplamente utilizado nos sistemas computacionais, pois o modelo tradicional tornou-se ineficiente e custoso para os usuários, que precisavam gerenciar e fornecer diversas informações em diferentes sistemas e provedores de serviços [6].

Um desafio recorrente associado a essa evolução é a questão da privacidade das informações. Os usuários frequentemente não têm o direito de determinar como e por quanto tempo suas informações serão manipuladas por diversas organizações, o que idealmente deveria ser possível em um cenário mais adequado [6, 11].

2.3 SSI

Com o aumento significativo nos incidentes de vazamento de identidades digitais, torna-se evidente a ineficácia de alguns métodos existentes de gerenciamento de identidades. Diante desse cenário, observa-se uma crescente busca por abordagens mais seguras, com foco na preservação da privacidade. Nesse contexto, surge o SSI [1].

Os elementos fundamentais do SSI incluem a ênfase na ampliação do controle do usuário sobre seus dados pessoais e na redução da dependência de serviços oferecidos por grandes corporações, como Google, Microsoft, entre outras, as quais atualmente detêm o controle da maioria das identidades digitais [2, 12]. O SSI pode ser caracterizado por outros atributos [2]:

- O usuário detém o controle de suas identidades digitais;
- O usuário possui acesso absoluto aos seus dados;
- Transparência nos sistemas e algoritmos utilizados;
- Identidades digitais persistentes e portáveis.
- Garantia da proteção dos direitos pessoais.

Há dois componentes relevantes no contexto de SSI, são eles: Credenciais Verificáveis (VCs, do inglês *Verifiable Credentials*) e os Identificadores Descentralizados (DIDs, do inglês *Decentralized Identifiers*) [13], os quais serão abordados nas seções 2.4 e 2.5, respectivamente.

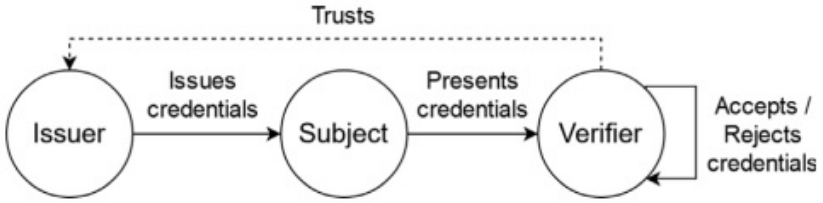

Figura 1 – Demonstração do funcionamneto do SSI.

Fonte: adaptado de [13]

A Figura 1 ilustra o processo de funcionamento do SSI e seus componentes. O processo se inicia com uma entidade emissora (*issuer*), que tem a autoridade para emitir e assinar VCs. Essas credenciais são emitidas em nome de um assunto (*subject*), que pode ser uma pessoa, uma organização ou um objeto, dependendo do contexto de uso. O papel do issuer é decisivo, pois sua confiabilidade e autenticidade fornecem a base para a validade das credenciais emitidas. Uma vez emitidas, as VCs são atribuídas a um indivíduo (*holder*), que na maioria das vezes é o próprio assunto a quem as credenciais se referem. O holder é responsável por armazenar suas VCs de maneira segura, geralmente em uma carteira digital, e apresentá-las conforme necessário para provar sua identidade, qualificações ou propriedades. Quando um holder deseja acessar serviços ou comprovar uma informação, ele deve apresentar suas VCs a uma entidade verificadora (*verifier*). A função do verifier é examinar as credenciais apresentadas, validar a assinatura digital do issuer para garantir sua autenticidade e, com base nisso, decidir aceitar ou recusar as credenciais. Esta etapa assegura que apenas VCs válidas e emitidas por entidades confiáveis sejam aceitas [13].

Detalhando um exemplo em que se aplica o uso de SSI: após a compra de veículo, uma concessionária atua como o orgão emissor (issuer) ao criar uma credencial verificável (VC) que certifica a compra. Esta credencial contém detalhes importantes sobre o veículo, como descrição, modelo, cor, chassi, etc. Essencialmente, o veículo é o assunto (subject) da credencial, e o comprador é o titular (holder) dessa credencial. O comprador, agora titular da VC, armazena essa credencial de forma segura, em uma carteira digital protegida por criptografia. Quando o titular deseja emplacar o veículo, ele se dirige ao Departamento Estadual de Trânsito (Detran), que neste cenário atua como a entidade verificadora (verifier). Para o procedimento de emplacamento, o titular apresenta a VC emitida pela concessionária. O Detran, então, verifica a autenticidade da credencial, con-

firmando a validade da assinatura digital da concessionária e as informações contidas na VC.

Uma vez que a credencial é verificada e aceita pelo Detran, o veículo pode ser oficialmente emplacado. Este passo finaliza o processo de transferência de propriedade (no sentido administrativo) e legaliza o veículo para uso em vias públicas, tudo isso facilitado pela troca segura e verificável de informações digitais.

Ultimamente tem-se observado um aumento significativo nas plataformas de SSI [1], entre as quais se destacam o Blockstack [14], uma plataforma open-source de nomeação e armazenamento descentralizado construída com tecnologia Blockchain. A UPort[5] constitui-se como uma framework de SSI baseada na rede blockchain pública da Ethereum. Já a SelfKey[6] é uma outra rede SSI que proporciona aos usuários um maior controle sobre seus dados pessoais, garantindo que apenas o mínimo necessário de informações seja compartilhado.

Conforme aumenta-se as discussões sobre SSI, nota-se que há muitos desafios a serem enfrentados, como por exemplo [1]:

- O gerenciamento de chave: Nos sistemas tradicionais de gerenciamento de chave, o controle dos dados e chaves são de responsabilidade do provedor, já no SSI, é o usuário que detém suas chaves de acesso, portanto, caso o mesmo perca essas chaves, haverá perda de informações irrecuperáveis.
- Confiabilidade dos dados: A comunicação entre os componentes de um sistema baseado em SSI deve ser implementada de maneira que impeça a interceptação de dados transmitidos de um componente para outro por terceiros, garantindo assim a segurança e confiabilidade do sistema. Além disso, deve haver validações rigorosas para prevenir fraudes na etapa de emissão de credenciais.
- Comercialização: Por ser uma novidade e estar em expansão, algumas entidades podem ficar relutantes quanto a adoção do SSI, por isso podem necessitar de suporte financeiro de algum serviço ou grande corporação para a adoção desta tecnologia.

2.4 Tecnologia VC

Credencial verificável (VC, do inglês *Verifiable Credential*) pode representar exatamente as mesmas informações de uma credencial física, uma VC faz o uso de assinaturas digitais que provam criptograficamente quem a emitiu [1] e [15]. No contexto físico, uma credencial pode ser definida conforme [15]:

[5] <https://www.uport.me>
[6] <https://selfkey.org>

- Informações para Identificação de um Indivíduo: incluem elementos como fotografia, nome e CPF. Esses dados servem para distinguir claramente uma pessoa das demais, garantindo sua identificação de forma precisa e confiável.

- Identificação do Órgão Emissor: refere-se às entidades responsáveis pela emissão de documentos oficiais que validam diversas informações. Exemplos destes órgãos incluem o Instituto de Identificação do Paraná (IIPR) e o Departamento Estadual de Trânsito (Detran). Estes documentos emitidos contêm detalhes que apontam para a origem e a autoridade do órgão que os forneceu, assegurando sua autenticidade e confiabilidade.

- Tipo da Credencial: como Carteira Nacional de Habilitação (CNH), cartão do Sistema Único de Saúde (SUS) ou passaporte, define a natureza e o escopo das informações que ela contém. Cada uma dessas credenciais carrega consigo atributos específicos e serve para comprovar distintas competências ou identificações do portador.

- Atributos do Indivíduo Afirmados pelo Órgão Emissor: constituem elementos básicos na validação da capacitação e identidade do mesmo. Tais atributos incluem, por exemplo, a categoria da habilitação, o número de identificação e a nacionalidade. Essas informações são conferidas pelo órgão emissor, servindo como meio de certificar as qualificações e a identidade do indivíduo.

- Evidência Relatando Como a Credencial Foi Designada: refere-se à documentação ou informações que atestam o processo pelo qual a credencial foi atribuída ou concedida. Essa evidência fornece detalhes sobre os procedimentos, critérios ou eventos que levaram à emissão da credencial. Como por exemplo, registros de transações, aprovações, verificações ou qualquer outra forma de documentação que esclareça como a credencial foi concedida. Essa informação é importante para validar a legitimidade e a autenticidade da credencial, permitindo uma compreensão transparente do processo de designação associado a ela.

- Restrições da Credencial: englobam limitações específicas impostas ao seu uso e validade. Exemplos notáveis incluem o período de validade da credencial e os termos de uso da mesma, que determinam as condições sob as quais a credencial pode ser utilizada. Estas restrições são fundamentais para garantir a aplicação correta e segura das credenciais dentro de seus contextos previstos.

O indivíduo (holder) que detém VC tem a capacidade de gerar Apresentações Verificáveis (VPs, do inglês *Verifiable Presentations*) e compartilhá-las com as entidades verificadoras com o intuito de comprovar efetivamente que possui VC com características

específicas. Tanto a VC quanto as VPs podem ser transmitidas de maneira ágil, conferindo-lhes maior conveniência em comparação com suas contrapartes físicas, especialmente ao tentar estabelecer um nível de confiança à distância [15]. Na Figura 2 é ilustrado um exemplo do funcionamento da VC:

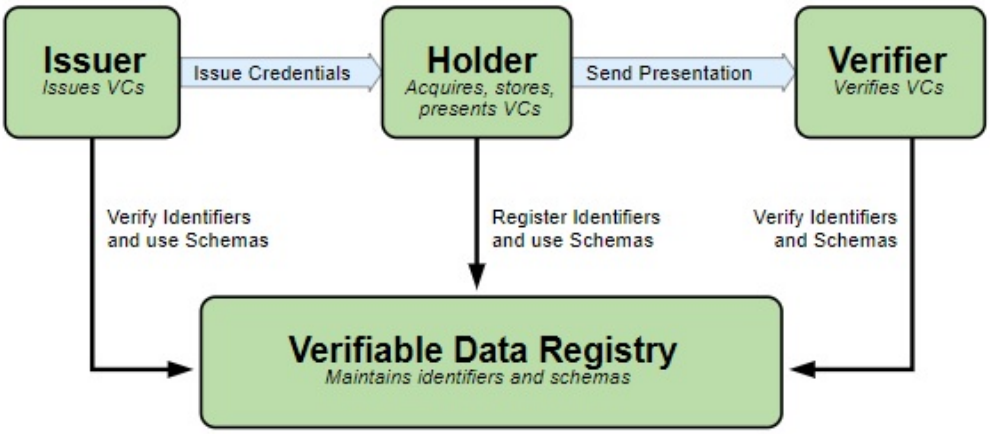

Figura 2 – Exemplo de funcionamento do VC.

Fonte: adaptado de [15]

Esclarecendo o fluxograma presente na Figura 2:

- **Holder:** Refere-se a um indivíduo que pode possuir uma ou mais VCs e gerar VPs para essas credenciais. Exemplos de holders podem incluir estudantes, funcionários e clientes, evidenciando a variedade de contextos nos quais os indivíduos podem ser detentores de VCs, cada uma representando distintas características ou afirmações sobre o titular.

- **Issuer:** Desempenha o papel de atribuir a propriedade sobre um ou mais assuntos (subjects), por meio da criação de VCs e sua subsequente transmissão para um holder. Exemplos ilustrativos dessa atuação incluem a atribuição de propriedade de um veículo a um indivíduo ou a atribuição de um CPF a uma pessoa (neste cenário, o subject da VC faz referência ao holder), entre outras possibilidades. São exemplos de entidades que executam essa função: organizações sem fins lucrativos, corporações e órgãos governamentais. Essas entidades, ao criar e emitir VCs, contribuem para a construção de um sistema que permite a representação confiável de informações sobre indivíduos e entidades em formatos digitais verificáveis. Esse processo apoia a facilitação da troca segura de informações em diversos contextos, destacando a versatilidade e a utilidade dessa abordagem em diferentes setores e organizações.

- **Subject:** É a entidade sobre a qual é exercida propriedade, pode se referir a diferentes objetos ou sujeitos, como animais ou veículos. Em muitas situações, o holder

da VC é também o subject, no entanto, em certos casos, essa relação pode ser distinta. Um exemplo ilustrativo é quando um pai atua como holder, detendo a VC que representa informações sobre uma criança, que é o subject. Nesse cenário, a VC não está diretamente vinculada ao próprio holder, mas sim a um terceiro, destacando a flexibilidade e adaptabilidade desse modelo de gerenciamento de identidades em situações diversas.

- **Verifier:** Responsável por receber uma ou mais VCs, possivelmente dentro de uma Apresentação Verificável (VP) para processamento. Essa função envolve a verificação e validação das informações contidas nas VCs, garantindo assim a autenticidade e confiabilidade dos dados apresentados. Em ecossistemas onde diferentes indivíduos possuem diferentes permissões, a validação das VCs é utilizada para garantir a integridade e autorização adequada desses indivíduos. Da mesma forma, em sites, a verificação de VCs pode ser empregada para fortalecer a autenticação dos usuários, promovendo a segurança e confiança nas transações e interações online.
- **Verifiable Data Registry (VDR):** É um sistema ou uma rede que possui como função mediar a criação e a verificação de identificadores, como chaves, esquemas de VCs, chaves públicas do emissor, etc., que são fundamentais para o uso de VCs, como por exemplo bancos de dados descentralizados, redes ponto a ponto (P2P, do inglês *peer-to-peer*), bancos de dados governamentais ou outras formas de armazenamento confiável. Em resumo, esse sistema mantém identificadores e esquemas, fornecendo uma infraestrutura fundamental para a operação de credenciais digitais.

Após a definição dos termos, o funcionamento da VC é delineado da seguinte maneira: um emissor acessa o VDR e verifica os identificadores, fazendo uso dos esquemas disponíveis. Sua principal função é, então, emitir VCs para o holder. O holder, por sua vez, adquire essas VCs, armazena no VDR e apresenta VPs ao verificador. O verificador, ao receber VCs ou VPs, verifica essas credenciais acessando o VDR e conferindo os identificadores e esquemas pertinentes [15].

2.5 Tecnologia DID

Organizações, provedoras de serviços e indivíduos fazem extenso uso de identificadores únicos em uma variedade significativa de contextos diários. Estes identificadores desempenham o papel fundamental de servir como endereços e meios de comunicação, abrangendo categorias como números de telefone, nomes de usuário, CPF, números de documentos como passaportes, carteiras de habilitação e até identificadores de produtos, como números de série [16].

É importante observar que a grande maioria desses identificadores não está sob nosso controle direto. Frequentemente, esses identificadores são emitidos por autoridades externas que determinam quem ou o que será referenciado por eles e estabelecem as condições sob as quais podem ser revogados[7]. Essa dinâmica ressalta a dependência de entidades externas no que diz respeito à atribuição e gestão desses identificadores essenciais na vida cotidiana [16].

O Identificador Descentralizado (DID, do inglês *Decentralized Identifier*) é uma tecnologia desenvolvida pelo World Wide Web Consortium (W3C) e desempenha um papel significativo no contexto do SSI [1]. Este novo tipo de identificador viabiliza uma identidade digital verificável e descentralizada, sendo que um DID pode ser atribuído a qualquer entidade, como uma pessoa, uma organização, um modelo de dados, entre outros. A referência associada a um DID é determinada pelo seu controlador [16].

O DID surgiu como uma alternativa aos identificadores centralizados, promovendo o desacoplamento de registros centralizados, provedores de identidade e autoridades de certificação. Seu design permite que o controlador de um DID comprove o controle sobre si mesmo sem depender da autorização de terceiros. Essa comprovação é realizada por meio de assinaturas digitais, que funcionam como prova criptográfica. Em resumo, o DID é um recurso uniforme de identificação (URI, do inglês *Uniform Resource Identifier*) que associa uma entidade de DID a um documento de DID, possibilitando interações confiáveis envolvendo essa entidade [16].

A Figura 3 mostra os principais componentes da arquitetura DID.

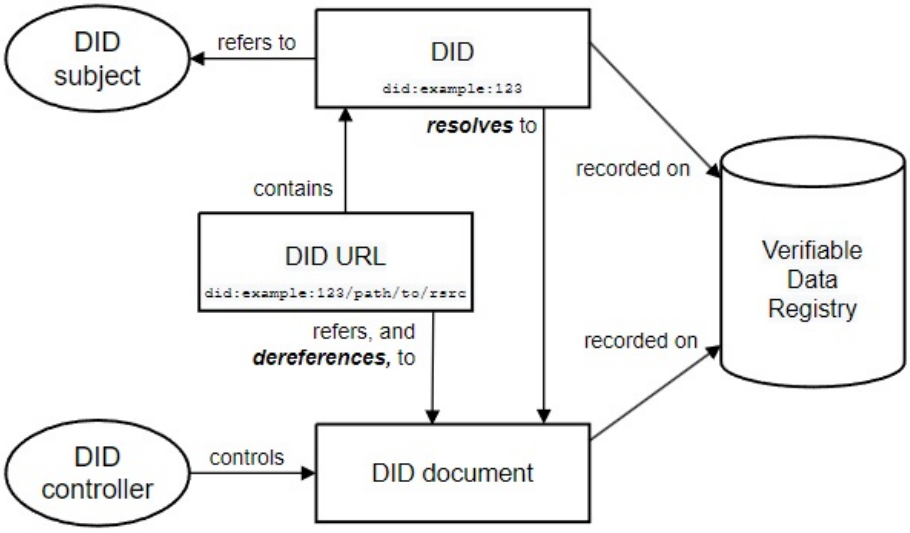

Figura 3 – Visão geral da arquitetura DID e a relação dos componentes básicos.

Fonte: adaptado de [16]

[7] <https://www.dock.io/post/decentralized-identifiers>

Na arquitetura do DID, são identificados seis componentes principais:

- **DID:** É representado por uma cadeia de caracteres simples que consiste em três partes distintas:

  1. Identificador de Esquema DID: Este identificador representa o esquema ao qual o identificador está vinculado. Ela proporciona um contexto para a interpretação do DID.
  2. Identificador do Método DID: Este componente define a metodologia ou o processo específico usado para a criação, resolução e operação do DID.
  3. Identificador do Método Específico: Este componente refere-se a um identificador único e específico associado ao método escolhido, fornecendo informações adicionais sobre a identidade representada.

  A Figura 4 mostra um exemplo simples de um DID.

Figura 4 – Exemplo simples de um DID.

Fonte: adaptado de [16]

- **DID URL:** Representa uma extensão da sintaxe do DID básico, permitindo a incorporação de outros padrões de URI. Essa extensão possibilita a inclusão de elementos como caminho (path) para localizar recursos específicos associados ao DID.
- **DID Subject:** Refere-se à entidade a que um DID faz referência, sendo possível que essa entidade seja o próprio controlador do DID.
- **DID Controller:** São entidades com a capacidade de modificar um documento DID. Essas entidades podem ser indivíduos ou organizações, e a habilidade de alteração é assegurada pelo uso de chaves criptográficas. Esse mecanismo proporciona uma camada adicional de segurança e controle sobre a gestão dos documentos DID, garantindo que apenas entidades autorizadas possam efetuar alterações nesses registros digitais.
- **Verifiable Data Registries (VDR):** São sistemas cuja função principal é intermediar o registro de DIDs. Exemplos desses sistemas incluem bancos de dados descentralizados, redes P2P e outras formas de armazenamento confiável.

- **DID Document:** É um registro que contém informações associadas a um DID. Essas informações geralmente incluem uma chave de criptografia pública ou serviços utilizados para interação com o *DID subject*.

Após a definição desses termos, o funcionamento do DID ocorre da seguinte maneira: o *DID controller* exerce controle sobre um *DID Document*, o qual é referenciado por uma *DID URL*. Este documento é registrado em um *VDR*. A *DID URL*, por sua vez, contém um DID, que faz referência ao *DID subject*. Existe uma resolução que leva ao *DID Document*, o qual também é armazenado em um *VDR*. Esse processo cria uma interconexão entre os elementos fundamentais do sistema DID, permitindo a gestão eficiente e segura dessas identidades digitais verificáveis.

Voltando ao exemplo da compra de um carro e seu emplacamento: antes de emitir a VC, a concessionária criará o DID para a transação e gerará um DID Document, que conterá informações como a chave de criptografia pública e os serviços associados ao veículo. A concessionária atua como DID Controller, pois é a única que pode modificar este DID Document. O DID Document será registrado no VDR, garantindo a verificabilidade e imutabilidade do DID.

Após a concessionária emitir a VC que certifica a compra do veículo, este se torna o DID Subject, ou seja, a entidade referenciada pelo DID. O comprador, que é o holder, receberá a VC e o DID. Quando o Detran, atuando como verifier, for realizar o emplacamento do veículo, o comprador deverá fornecer o DID. O Detran utilizará a DID URL fornecida pelo comprador para acessar o DID Document associado ao veículo e à transação de compra. Esse acesso será feito através do VDR. Dessa forma, o Detran verifica a autenticidade da credencial, confirmando a validade da assinatura digital da concessionária.

2.6 Blockchain

Blockchain consiste em uma rede P2P onde os dados são organizados em uma estrutura de dados composta por blocos. Esses blocos são abstrações utilizadas para representar os conjuntos de dados na rede. Toda transação na rede possui um registro que é copiado e distribuído em toda a rede [17, 18].

A Figura 5 mostra um exemplo de uma Blockchain.

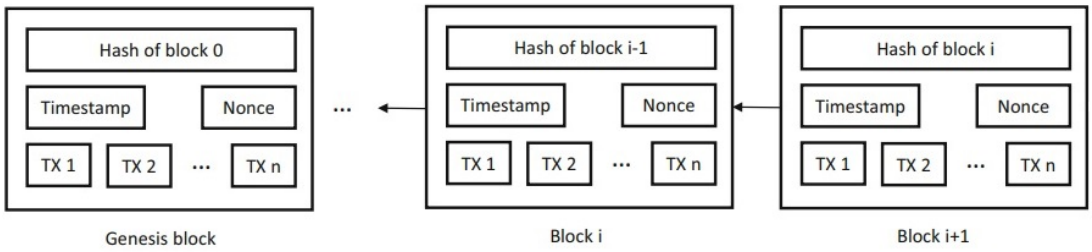

Figura 5 – Exemplo simples de uma Blockchain.

Fonte: adaptado de [18]

Cada novo bloco adicionado à blockchain estende a cadeia, formando um registro completo do histórico de transações. A validação dos blocos é realizada pela rede por meio de mecanismos criptográficos. Cada bloco contém múltiplas **transações**, um carimbo de data/hora (**Timestamp**), o valor do **hash** do bloco anterior, e um **Nonce**, que é um número aleatório usado para verificação do hash. Dessa forma é assegurado a integridade de toda a blockchain até o primeiro bloco, conhecido como "bloco gênese". Os valores de hash são únicos, o que permite a detecção eficaz de tentativas de fraude, já que qualquer alteração em um bloco modifica imediatamente o valor do hash correspondente [17].

Para que um bloco seja adicionado à cadeia, a maioria dos nós da rede deve concordar sobre a validade das transações e do próprio bloco. Essa "concordância"é alcançada por meio de um mecanismo de consenso. Este mecanismo é um processo pelo qual a maioria, ou em alguns casos todos os validadores da rede, chegam a um acordo sobre o estado de uma transação na rede. Trata-se de um conjunto de regras e procedimentos que permite manter um conjunto coerente de fatos entre vários nós participantes da rede. Novas transações não são adicionadas automaticamente à rede, em vez disso, o processo de consenso assegura que essas transações sejam armazenadas em um bloco por um determinado tempo antes de serem transferidas para a blockchain, pois as informações na blockchain não podem ser alteradas após adicionadas [17, 19].

A tecnologia da Blockchain foi introduzida em outubro de 2008 como parte da proposta do bitcoin, uma moeda virtual. O bitcoin foi a primeira aplicação da tecnologia Blockchain [19]. Posteriormente, surgiram outras moedas virtuais que fazem uso de Blockchain devido à sua transparência e seu funcionamento como um "livro de registros"que pode gravar transações de forma eficiente entre usuários da rede. Essas transações são verificáveis e permanentes [19].

Há uma ampla variedade de áreas que podem se beneficiar do uso de Blockchain, tais como saúde, serviços financeiros, entretenimento e mídia, gestão de identidade, entre outras [20]. Na saúde, facilita o compartilhamento seguro de dados entre organizações,

melhorando a segurança das informações dos pacientes [21]. No setor financeiro, grandes instituições como Bank of America, JPMorgan e Nasdaq exploram o Blockchain para substituir transações manuais em áreas como câmbio, investimentos e apólices de seguro [19]. Na indústria do entretenimento e mídia, a imutabilidade dos registros proporcionada pelo Blockchain oferece uma proteção mais segura dos direitos autorais [17].

Além disso, o Blockchain é uma aplicação promissora no gerenciamento de identidade, permitindo aos usuários criar uma identidade digital confiável e segura, substituindo nomes de usuário e senhas por uma identificação única baseada em Blockchain. Com isso, os usuários podem assinar documentos digitais, fazer login em diferentes sites e realizar transações bancárias de forma mais segura [18].

A ascensão da tecnologia blockchain nos últimos anos também tem sustentado outros conceitos propostos na literatura, como o de contratos inteligentes (do inglês, *Smart Contracts*). Estes combinam protocolos computacionais com interfaces de usuário para executar os termos de um contrato. Essa abordagem inovadora tem o potencial de substituir intermediários, como advogados e bancos, que geralmente estão envolvidos em contratos para transações de ativos. Os contratos inteligentes também podem ser utilizados para controlar a propriedade de bens, como casas, automóveis, ações ou até mesmo direitos de acesso [17].

Em resumo, a tecnologia Blockchain tem o potencial de se tornar o sistema de registros utilizado para todas as transações atuais [19].

3 MATERIAIS E MÉTODOS

3.1 Proposta

O presente trabalho propõe um modelo que utiliza o conceito de SSI para facilitar a prestação de serviços públicos, com foco específico em serviços que oferecem benefícios e exigem credenciais para comprovar informações necessárias à obtenção desses benefícios. A implementação deste modelo visa identificar e discutir os desafios associados ao SSI, além de responder às seguintes questões:

- Quais ferramentas são essenciais para a implementação de uma solução baseada em SSI?
- Quais são os principais desafios associados à implementação de uma solução baseada em SSI?
- Como uma solução baseada em SSI se diferencia de uma solução centralizada?
- Qual é o nível de aceitação por parte dos indivíduos em relação ao uso do SSI?

Com este trabalho, busca-se não apenas explorar as vantagens do uso de SSI na prestação de serviços públicos, mas também avaliar as dificuldades práticas e a receptividade dos usuários em relação a esta abordagem inovadora de gestão de identidades.

3.2 Caso de Uso

4 CONCLUSÃO

REFERÊNCIAS

[1] SOLTANI, R.; NGUYEN, U. T.; AN, A. A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, Hindawi Limited, v. 2021, p. 1–26, 2021.

[2] DER, U.; JÄHNICHEN, S.; SÜRMELI, J. Self-sovereign identity − opportunities and challenges for the digital revolution. *arXiv preprint arXiv:1712.01767*, 2017.

[3] COUTO, E. Educação e redes sociais digitais: privacidade, intimidade inventada e incitação à visibilidade. *Em Aberto*, v. 28, n. 94, 2015.

[4] REIS, É. V. B.; NAVES, B. T. de O. O meio ambiente digital e o direito à privacidade diante do big data. *Veredas do Direito*, v. 17, n. 37, p. 145–167, 2020.

[5] KORMANN, D. P.; RUBIN, A. D. Risks of the passport single signon protocol. *Computer networks*, Elsevier, v. 33, n. 1-6, p. 51–58, 2000.

[6] WANGHAM, M. S. et al. Gerenciamento de identidades federadas. *Sociedade Brasileira de Computação*, 2010.

[7] ORACLE. *Identity Management*. Acessado em 23 de Fevereiro de 2024. Disponível em: <https://www.oracle.com/br/security/identity-management/what-is-iam/>.

[8] ZWITTER, A. J.; GSTREIN, O. J.; YAP, E. Digital identity and the blockchain: Universal identity management and the concept of the "self-sovereign" individual. *Frontiers in blockchain*, Frontiers Media S.A, v. 3, 2020. ISSN 2624-7852.

[9] GUARDIAN, T. *Marriott to be fined nearly £100m over GDPR breach*. Acessado em 30 de Abril de 2024. Disponível em: <https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico>.

[10] MULAJI, S. M.; ROODT, S. Factors affecting organisations' adoption behaviour toward blockchain-based distributed identity management: The sustainability of self-sovereign identity in organisations. *Sustainability*, v. 14, n. 18, 2022. ISSN 2071-1050. Disponível em: <https://www.mdpi.com/2071-1050/14/18/11534>.

[11] ALPÁR, G.; HOEPMAN, J.-H.; SILJEE, J. The identity crisis. security, privacy and usability issues in identity management. *arXiv preprint arXiv:1101.0427*, 2011.

[12] LOCKL, J. et al. The paradoxical impact of information privacy on privacy preserving technology: The case of self-sovereign identities. *International Journal of Innovation and Technology Management*, v. 20, n. 04, p. 2350025, 2023. Disponível em: <https://doi.org/10.1142/S0219877023500256>.

[13] Di Francesco Maesa, D. et al. Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge. *Journal of Network and Computer Applications*, v. 212, p. 103577, 2023. ISSN 1084-8045. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804522002181>.

[14] ALI, M. et al. Blockstack: A new internet for decentralized applications. *Doylestown, United States*, 2017.

[15] SPORNY, M. et al. *Verifiable Credentials Data Model v2.0*. Acessado em 19 de Fevereiro de 2024. Disponível em: <https://www.w3.org/TR/vc-data-model-2.0/>.

[16] SPORNY, M. et al. *Decentralized Identifiers (DIDs) v1.0*. Acessado em 19 de Fevereiro de 2024. Disponível em: <https://www.w3.org/TR/did-core/>.

[17] NOFER, M. et al. Blockchain. *Business information systems engineering*, Springer Fachmedien Wiesbaden, Wiesbaden, v. 59, n. 3, p. 183–187, 2017. ISSN 2363-7005.

[18] JAVAID, M. et al. A review of blockchain technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, v. 2, n. 3, p. 100073, 2022. ISSN 2772-4859. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2772485922000606>.

[19] IANSITI, M.; LAKHANI, K. R. et al. The truth about blockchain. *Harvard business review*, Boston, MA, USA:, v. 95, n. 1, p. 118–127, 2017.

[20] STRAWN, G. Blockchain. *IT Professional*, v. 21, n. 1, p. 91–92, 2019.

[21] TANDON, A. et al. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Computers in Industry*, v. 122, p. 103290, 2020. ISSN 0166-3615. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0166361520305248>.