

**UNIVERSIDADE DO ESTADO DE SANTA CATARINA - UDESC  
CENTRO DE CIÊNCIAS TECNOLÓGICAS - CCT  
MESTRADO EM COMPUTAÇÃO APLICADA**

**JANAÍNA FONTANA BIFFI DUARTE**

**COTTONTRUST: CONFIABILIDADE E RASTREABILIDADE NA  
CADEIA PRODUTIVA DO ALGODÃO USANDO IDENTIDADES  
DIGITAIS AUTOSSOBERANAS**

**JOINVILLE**

**2024**

**JANAÍNA FONTANA BIFFI DUARTE**

**COTTONTRUST: CONFIABILIDADE E RASTREABILIDADE NA  
CADEIA PRODUTIVA DO ALGODÃO USANDO IDENTIDADES  
DIGITAIS AUTOSSOBERANAS**

Dissertação submetida ao Programa de Pós-Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Dr. Maurício Aronne Pilon

**JOINVILLE**

**2024**

**Ficha catalográfica elaborada pelo programa de geração automática da  
Biblioteca Universitária Udesc,  
com os dados fornecidos pelo(a) autor(a)**

Duarte, Janaína Fontana Biffi

COTTONTRUST: confiabilidade e rastreabilidade na cadeia produtiva do algodão usando identidades digitais autossobranas / Janaína Fontana Biffi Duarte. -- 2024.  
117 p.

Orientador: Maurício Aronne Pillon  
Dissertação (mestrado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada, Joinville, 2024.

1. Identidade digital autossobranas. 2. Blockchain. 3. Hyperledger Indy. 4. Cadeia produtiva do algodão. I. Aronne Pillon, Maurício. II. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada. III. Título.

**JANAÍNA FONTANA BIFFI DUARTE**

**COTTONTRUST: CONFIABILIDADE E RASTREABILIDADE NA CADEIA  
PRODUTIVA DO ALGODÃO USANDO IDENTIDADES DIGITAIS  
AUTOSSOBERANAS**

Esta dissertação foi julgada adequada para a obtenção do título de **Mestre em Computação Aplicada** área de de concentração em "Sistemas de Computação", e aprovada em sua forma final pelo Curso de Mestrado em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina.

**Banca Examinadora:**

---

**Dr. Maurício Aronne Pillon**  
Orientador

---

**Dr. Guilherme Piêgas Koslovski**  
CCT/UDESC

---

**Dr. Ricardo José Pfitscher**  
UFSC

---

**Dr. Charles Christian Miers**  
CCT/UDESC

Joinville, 31 de janeiro de 2024

Aos meus pais Odilo e Olga, ambos do outro lado da vida, com todo o meu amor e gratidão...

## **AGRADECIMENTOS**

Agradeço, em especial, ao meu orientador professor Dr. Maurício Aronne Pilon por aceitar conduzir o meu trabalho de pesquisa e por me inspirar a ir mais longe. Eu gostaria que todos os alunos tivessem um professor que acredita neles, como você acreditou em mim. Muito obrigada!

Ao professor Dr. Ricardo Antonio de Simone Zanon pelo incentivo para que eu iniciasse o curso. Talvez eu não tivesse tomado essa decisão sem a sua motivação. Agradeço também às professoras Dra. Avanilde Kemczinski e Dra. Isabela Gasparini, que me orientaram e auxiliaram no início dessa jornada.

Aos meus filhos e ao meu marido, agradeço pela presença amorosa e pelo apoio incondicional que foram a base que me manteve centrada ao longo de toda a trajetória.

Agradeço à minha amiga e braço direito, Zerli Aparecida Ramilio, pelo suporte essencial e dedicação, orando e proporcionando tranquilidade, que foram elementos preciosos em cada passo do caminho.

"The Internet was built without a way to know who and what you are connecting to."  
(Kim Cameron)

## RESUMO

Uma identidade digital é a representação de uma entidade presente no ciberespaço capaz de identificar, de forma única, uma entidade (dispositivo, pessoa ou coisa). Associar uma identidade digital confiável à uma entidade virtual garante a identificação dos envolvidos em transações e manipulações de dados. Nesse sentido, o modelo de Identidade Digital Autossoberana (SSI) é um novo paradigma que delega a gerência dos dados à própria entidade, a quem a identidade pertence. A SSI é descentralizada e independente de qualquer organização certificadora, sendo, deste modo, naturalmente mais escalável. Nesse contexto, a hipótese deste trabalho é que o uso de identidades autossoberanas possa ser alavancado a partir da sua aplicação no ecossistema que envolve a cadeia produtiva do algodão. Dessa forma, propõe-se um projeto de arquitetura e desenvolvimento de um sistema transparente e descentralizado, que visa proporcionar recursos para a verificação de selos de certificação e para a rastreabilidade do algodão. Além disso, busca estabelecer confiança nas informações apresentadas e nas transações realizadas entre os diversos participantes dessa cadeia, caracterizada por sua complexidade e geografia dispersa. Ao instanciar a solução em uma prova de conceito, é demonstrada a viabilidade da abordagem proposta e avaliada sua adequação para resolver problemas que envolvem transações dessa natureza.

**Palavras-chaves:** identidade digital autossoberana, blockchain, hyperledger indy, cadeia produtiva do algodão

## ABSTRACT

A digital identity is the representation of an entity in cyberspace capable of uniquely identifying a subject (device, person, or thing). Associating a reliable digital identity with a virtual entity ensures the identification of those involved in transactions and data manipulations. In this sense, the Self-Sovereign Identity (SSI) model is a new paradigm that delegates data management to the entity to whom the identity belongs. SSI is decentralized and independent of any certifying authority, making it naturally more scalable. In this context, the hypothesis of this work is that the use of self-sovereign identities can be leveraged through their application in the ecosystem involving the cotton supply chain. Therefore, a project for the architecture and development of a transparent and decentralized system is proposed, aiming to provide resources for the verification of certification seals and the traceability of cotton. Furthermore, it seeks to establish trust in the information presented and transactions conducted among the various participants in this chain, characterized by its complexity and dispersed geography. By instantiating the solution in a proof of concept, the feasibility of the proposed approach is demonstrated, and its suitability for solving problems involving transactions of this nature is evaluated.

**Key-words:** self-sovereign identity, blockchain, hyperledger indy e cotton supply chain.

## LISTA DE ILUSTRAÇÕES

Figura 1 – Ecossistema das Credenciais Verificáveis . . . . .	24
Figura 2 – Propriedades das Credenciais e Apresentações Verificáveis . . . . .	25
Figura 3 – Triângulo da Confiança no SSI . . . . .	27
Figura 4 – Formato geral de um DID . . . . .	28
Figura 5 – Relacionamento entre DID, Documento DID e Assunto DID . . . . .	28
Figura 6 – Segundo Triângulo da Confiança do SSI . . . . .	31
Figura 7 – Pilha SSI . . . . .	33
Figura 8 – Protocolo de conexão . . . . .	35
Figura 9 – Protocolo de emissão da credencial . . . . .	36
Figura 10 – Protocolo de apresentação da prova . . . . .	37
Figura 11 – Cadeia Produtiva do Algodão - Visão Macro dos Grandes Blocos. . . . .	40
Figura 12 – Cadeia Produtiva do Algodão (em destaque as fases de beneficia- mento e comercialização de fardos de algodão em pluma). . . . .	48
Figura 13 – Arquitetura do COTTONTRUST . . . . .	50
Figura 14 – Exemplo de DID Público da entidade Unidade de Beneficiamento de Algodão (UBA) . . . . .	51
Figura 15 – Documento do DID <i>did:mybc:TsiaIUyBJPxVBnz8w2B5gb</i> . . . . .	51
Figura 16 – Esquema de uma credencial referente ao CNPJ . . . . .	54
Figura 17 – Definição da credencial baseada no esquema da Figura 16 . . . . .	55
Figura 18 – Estrutura da credencial baseada na definição da Figura 17 . . . . .	55
Figura 19 – Estrutura de uma apresentação verificável . . . . .	56
Figura 20 – Prova de posse dos atributos . . . . .	57
Figura 21 – Dinâmica Funcional no COTTONTRUST - Triângulo da Confiança. . . . .	58
Figura 22 – Visão Geral do Funcionamento do COTTONTRUST . . . . .	64
Figura 23 – Diagrama de atividade do estabelecimento de conexão entre duas entidades . . . . .	67
Figura 24 – Esquemas e Credenciais . . . . .	68
Figura 25 – Diagrama de atividade do processo de Obtenção de Credenciais . . . . .	69
Figura 26 – Diagrama de atividade do processo de Apresentação e Verificação de Provas . . . . .	70
Figura 27 – Transações do tipo REG_ENTITY . . . . .	73
Figura 28 – Transações do tipo SELL_COTTON . . . . .	74
Figura 29 – Evolução dos Modelos de Gerenciamento de Identidade . . . . .	87
Figura 30 – Modelo de Gerenciamento de Identidade Isolado . . . . .	87
Figura 31 – Modelo de Gerenciamento de Identidade Centralizado . . . . .	88
Figura 32 – Modelo de Gerenciamento de Identidade Federado . . . . .	89

Figura 33 – Modelo de Gerenciamento de Identidade Centrado no Usuário . . . .	90
Figura 34 – Modelo de Gerenciamento de Identidade Autossoberano . . . . .	91
Figura 35 – Estrutura de um pedido à blockchain . . . . .	102
Figura 36 – Tipos de operações de escrita e de leitura . . . . .	103
Figura 37 – Visão geral do funcionamento do COTTONTRUST destacando o fluxo de trabalho relacionado ao caso de uso . . . . .	107
Figura 38 – Página de gestão de DIDs . . . . .	109
Figura 39 – Criação dos DIDs públicos utilizando <i>seeds</i> . . . . .	109
Figura 40 – Submissão do esquema "selo_de_certificacao" para a blockchain . .	110
Figura 41 – Submissão da definição de uma credencial para a blockchain . . . .	110
Figura 42 – Página de gestão de conexões . . . . .	111
Figura 43 – Criação do convite de conexão . . . . .	111
Figura 44 – Página de gestão de conexões - Convites . . . . .	112
Figura 45 – Utilização de convites . . . . .	112
Figura 46 – Conexão ativa entre o OCE e o FAD . . . . .	113
Figura 47 – Página de gestão da emissão de credenciais . . . . .	113
Figura 48 – Formulário de emissão de uma credencial . . . . .	114
Figura 49 – Página de gestão de credenciais do FAD . . . . .	115
Figura 50 – Página de gestão de apresentações de provas . . . . .	115
Figura 51 – Formulário de pedido de prova . . . . .	116
Figura 52 – Página de gestão de apresentações de provas do CMI . . . . .	116
Figura 53 – Página de gestão de apresentações de provas do FAD . . . . .	117
Figura 54 – CMI verifica a validade da prova . . . . .	117

## LISTA DE TABELAS

Tabela 1 – Funções Principais das Carteiras e Agentes Digitais . . . . .	30
Tabela 2 – Blocos de construção do SSI . . . . .	32
Tabela 3 – Critérios de Avaliação - Comparação entre os trabalhos relacionados.	47
Tabela 4 – Comparação entre os Modelos de Gerenciamento de Identidade . .	92
Tabela 5 – Benefícios da blockchain em SSI . . . . .	95
Tabela 6 – Comparação entre os <i>Frameworks</i> SSI . . . . .	99

## LISTA DE ABREVIATURAS E SIGLAS

<b>DID</b>	<i>Decentralized Identifier</i>
<b>DLT</b>	<i>Distributed Ledger Technology</i>
<b>GDPR</b>	<i>General Data Protection Regulation</i>
<b>IdM</b>	<i>Identity Management</i>
<b>IdP</b>	<i>Identity Provider</i>
<b>IPFS</b>	<i>InterPlanetary File System</i>
<b>ITU</b>	<i>International Telecommunication Union</i>
<b>ITU-T</b>	<i>Telecommunication Standardization Sector</i>
<b>LGPD</b>	Lei Geral de Proteção de Dados
<b>MAPA</b>	Ministério da Agricultura, Pecuária e Abastecimento
<b>MBA</b>	Mecanismo de Busca Acadêmica
<b>NIST</b>	<i>National Institute of Standards and Technology</i>
<b>NFT</b>	<i>Non-fungible tokens</i>
<b>PAD</b>	<i>Personal Authentication Device</i>
<b>PBS</b>	Pesquisa Bibliográfica Sistemática
<b>RDV</b>	Registro de Dados Verificável
<b>SP</b>	<i>Service Provider</i>
<b>SSI</b>	<i>Self-Sovereign Identity</i>
<b>UBA</b>	Unidade de Beneficiamento de Algodão
<b>W3C</b>	<i>World Wide Web Consortium</i>
<b>ZKP</b>	<i>Zero-Knowledge Proof</i>

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>16</b>
1.1	Objetivos	18
1.2	Estrutura do Texto	19
<b>2</b>	<b>IDENTIDADE DIGITAL AUTOSSOBERANA</b>	<b>20</b>
2.1	Arquitetura	22
<b>2.1.1</b>	<b>Credenciais Verificáveis</b>	<b>22</b>
<b>2.1.2</b>	<b>Triângulo da Confiança</b>	<b>26</b>
<b>2.1.3</b>	<b><i>Decentralized Identifiers (DIDs)</i></b>	<b>26</b>
<b>2.1.4</b>	<b>Carteiras e Agentes Digitais</b>	<b>29</b>
<b>2.1.5</b>	<b>Registro de Dados Verificável</b>	<b>29</b>
<b>2.1.6</b>	<b>Estruturas de Governança</b>	<b>29</b>
2.2	Resumindo os blocos de construção e definindo a Pilha SSI	30
2.3	Protocolos de Comunicação	34
<b>2.3.1</b>	<b>Protocolo de Conexão</b>	<b>34</b>
<b>2.3.2</b>	<b>Protocolo de emissão da credencial</b>	<b>35</b>
<b>2.3.3</b>	<b>Protocolo de apresentação verificável (provas)</b>	<b>37</b>
2.4	Considerações Parciais	38
<b>3</b>	<b>CADEIA PRODUTIVA DO ALGODÃO</b>	<b>40</b>
3.1	Etapas da Cadeia Algodoeira	40
3.2	Estudos Relacionados	42
<b>3.2.1</b>	<b>Definição dos Termos de Pesquisa</b>	<b>42</b>
<b>3.2.2</b>	<b>Seleção</b>	<b>43</b>
<b>3.2.3</b>	<b>Fontes</b>	<b>43</b>
<b>3.2.4</b>	<b>Análise</b>	<b>43</b>
<b>3.2.5</b>	<b>Execução</b>	<b>44</b>
<b>3.2.6</b>	<b>Elegibilidade</b>	<b>44</b>
3.3	Discussão	44
3.4	Considerações Parciais	47
<b>4</b>	<b>COTTONTRUST</b>	<b>48</b>
4.1	COTTON-CELL - Componentes e Estrutura	50
4.2	Funcionamento	56
4.3	COTTON-TRANSACTIONS	59

4.4	Considerações Parciais . . . . .	60
<b>5</b>	<b>EXPERIMENTAÇÃO E ANÁLISE DE RESULTADOS . . . . .</b>	<b>62</b>
5.1	Ambiente de Testes . . . . .	62
5.2	Protótipo . . . . .	63
5.3	Plano de Testes . . . . .	72
5.4	Discussão e Análise de Resultados . . . . .	72
5.5	Considerações Parciais . . . . .	74
<b>6</b>	<b>CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS . . . . .</b>	<b>75</b>
6.1	Produções . . . . .	76
	<b>REFERÊNCIAS . . . . .</b>	<b>78</b>
	<b>ANEXO A – IDENTIDADES DIGITAIS . . . . .</b>	<b>84</b>
A.1	Gerenciamento de Identidade . . . . .	85
A.2	Evolução dos Modelos de Gerenciamento de Identidade . . . . .	87
<b>A.2.1</b>	<b>Modelo Isolado . . . . .</b>	<b>87</b>
<b>A.2.2</b>	<b>Modelo Centralizado . . . . .</b>	<b>88</b>
<b>A.2.3</b>	<b>Modelo Federado . . . . .</b>	<b>88</b>
<b>A.2.4</b>	<b>Modelo Centrado no Usuário . . . . .</b>	<b>90</b>
<b>A.2.5</b>	<b>Modelo Autossoberano . . . . .</b>	<b>90</b>
A.3	Comparação entre os Modelos de Gerenciamento de Identidade . . . . .	91
	<b>ANEXO B – FRAMEWORKS SSI . . . . .</b>	<b>93</b>
B.1	Blockchain . . . . .	93
B.2	Blockchain e SSI . . . . .	95
B.3	Shocard . . . . .	95
B.4	Civic . . . . .	96
B.5	Sovrin . . . . .	96
B.6	uPort . . . . .	97
B.7	Hyperledger Indy, Aries e Ursa . . . . .	97
B.8	Comparação entre os principais <i>frameworks</i> SSI . . . . .	99
	<b>ANEXO C – HYPERLEDGER INDY . . . . .</b>	<b>101</b>
C.1	Indy Plenum . . . . .	101
C.2	Indy Node . . . . .	102
C.3	Indy SDK . . . . .	105
C.4	Aries Agent . . . . .	105

C.5	Ursa . . . . .	105
	<b>ANEXO D – CASO DE USO . . . . .</b>	<b>107</b>
D.1	Criação de Entidades . . . . .	108
D.2	Criação de DIDs . . . . .	108
D.3	Criação de esquemas e definições de credenciais . . . . .	109
D.4	Criação de conexões . . . . .	110
D.5	Emissão de uma credencial verificável . . . . .	113
D.6	Apresentação de uma prova . . . . .	114

## 1 INTRODUÇÃO

Uma cadeia produtiva é um conjunto de etapas consecutivas, ao longo das quais insumos sofrem algum tipo de transformação, até a constituição de um produto final e sua colocação no mercado (CHOPRA; MEINDL, 2001). Segundo o Ministério da Agricultura, Pecuária e Abastecimento (MAPA), a cadeia produtiva do algodão se caracteriza como uma das mais longas e complexas, sendo constituída por inúmeras etapas desde a produção da semente até o consumidor final (BUAINAIN et al., 2007). A natureza distribuída, internacional e competitiva da cadeia implica em várias partes independentes que podem não compartilhar confiança mútua. Essa falta de confiança entre os diversos elos demanda informações verificáveis sobre o produto e o processo produtivo. Nesse cenário, a transparência torna-se crucial, uma vez que não há uma entidade central que detenha a confiabilidade universal. Cada parte, devido à sua autonomia e competição, busca garantias tangíveis e informações claras para assegurar a qualidade e autenticidade ao longo de toda a extensão da cadeia algodoeira.

No que diz respeito à rastreabilidade, esta desempenha um papel significativo, tanto para a auditabilidade, quanto para a conformidade com os regulamentos desse mercado globalizado. A rastreabilidade remonta à década de 1930, quando os países europeus queriam provar a origem de bebidas de alta qualidade, como o champagne francês, tendo sua importância destacada nas últimas décadas devido a várias preocupações relacionadas à segurança alimentar, como a doença da encefalopatia espongiforme bovina e a gripe aviária (JOSEPH, 2001). Porém, é fato que, além da indústria alimentícia, outras indústrias também são afetadas devido aos problemas de segurança, proteção e qualidade dos produtos. Sob a perspectiva do consumidor, no que diz respeito ao algodão e outros produtos agrícolas, os selos de certificação, exercem uma função importante no sentido de aumentar a transparência ao longo das cadeias produtivas e informar ao consumidor sobre a qualidade, segurança e sustentabilidade do produto (GRUNERT; HIEKE; WILLS, 2014). No entanto, como esses selos são impressos nos produtos, podem ser facilmente falsificados, influenciando diretamente a confiabilidade.

Ademais, não há uma maneira fácil para os consumidores, ou outras partes da cadeia, verificarem essas informações. Exemplificadamente, na área de produtos orgânicos, os produtores buscam mostrar o ciclo de vida completo do produto. Todavia, a principal importância para os consumidores e outras partes é validar que o produto é de fato orgânico, o que não é possível nesse contexto. Portanto, faz-se necessário fornecer um meio confiável de verificar as alegações apresentadas pelos selos de certificação, fornecendo recursos de verificabilidade aos consumidores.

Dessa forma, essas questões justificam a necessidade da cadeia do algodão ser confiável e rastreável, bem como fornecer meios de auditar as informações dos produtos e verificar a autenticidade dos selos de certificação. Recentemente, muitos trabalhos de pesquisa investigaram o potencial da tecnologia blockchain [(COCCO; TONELLI; MARCHESI, 2021; AGRAWAL et al., 2021; HADER et al., 2022; SEZER; TOPAL; NURIYEV, 2022; MALIK et al., 2021)], para melhorar a integridade, fluxos de informação e rastreabilidade das cadeias produtivas, e assim contribuir para a transparência e segurança dos sistemas de gestão dessas cadeias. No entanto, essas soluções podem ser desafiadoras para organizações de pequena escala devido à lacuna digital, custos de implementação e habilidades necessárias, bem como não atende aos requisitos de verificabilidade e confiabilidade. Ademais, os regulamentos de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) e *General Data Protection Regulation* (GDPR), podem impactar a adoção da tecnologia blockchain para cadeias produtivas devido as questões de privacidade, na medida em que fornecem regras legais rígidas sobre armazenamento e processamento de dados sensíveis, que não devem ser armazenados na blockchain.

Quando se fala em confiança, descentralização de informações, privacidade, segurança e transparência, nos últimos anos, o modelo de *Self-Sovereign Identity* (SSI) emergiu como um novo paradigma descentralizando o controle e a posse das informações pessoais (SOLTANI; NGUYEN; AN, 2021). Baseado em credenciais verificáveis e identificadores descentralizados, surgiu da necessidade dos usuários terem controle absoluto e exclusivo de seus dados (WOLFF; HENRIQUES, 2021). No entanto, a aplicação mais comum da SSI concentra-se principalmente às identidades de indivíduos e dispositivos de IoT. Embora a literatura enfatize a ausência de restrições para estender a utilização da SSI para além do domínio pessoal ou da IoT, com benefícios potenciais para outras relações que demandam confiança, uma pesquisa não exaustiva não revelou autores que explorem seu uso em outros cenários.

Dessa forma, as preocupações acerca da confiança, rastreabilidade, verificabilidade e auditabilidade, inerentes à cadeia de produção do algodão, requerem uma abordagem inovadora para alcançar os requisitos desejados. Portanto, a questão primordial desta pesquisa é delineada como segue: "Como obter rastreabilidade e confiabilidade na cadeia produtiva do algodão, considerando os desafios relacionados à dispersão geográfica, complexidade da cadeia e diversidade das partes envolvidas, empregando os conceitos do modelo SSI?"

Esta questão de pesquisa está decomposta nas seguintes subquestões:

- I. Como criar um sistema de rastreabilidade totalmente transparente e descentralizado para cadeias produtiva do algodão?

- II. Como fornecer recursos de verificabilidade dos selos de certificação e laudos de classificação do algodão?
- III. Como prover confiança nas informações apresentadas e nas transações realizadas entre os participantes dessa cadeia extensa e internacional?

Nesse contexto, a hipótese deste trabalho é que o uso de identidades autossoberanas possa ser alavancado em outros cenários, a partir do seu uso no ecossistema que envolve a cadeia produtiva do algodão, beneficiando-se assim da independência, autenticidade e transparência já estabelecida para pessoas e dispositivos de IoT.

## 1.1 OBJETIVOS

Com base nesse cenário, o objetivo geral deste trabalho é realizar uma prova de conceito com o intuito de garantir a rastreabilidade, confiança e verificabilidade na cadeia produtiva do algodão. Por meio dessa prova de conceito, pretende-se investigar como a aplicação do SSI pode contribuir para melhorar a transparência e a segurança ao longo da cadeia produtiva do algodão, e explorar a sua utilização para permitir o rastreamento eficiente e confiável do produto.

Além disso, o objetivo é examinar como o SSI pode viabilizar a verificabilidade das informações e a realização de auditorias, fornecendo um sistema confiável para comprovar a autenticidade, a origem e a conformidade dos produtos de algodão ao longo de sua jornada na cadeia produtiva. Ao final desta prova de conceito, espera-se obter compreensão sobre a aplicação do SSI na cadeia produtiva do algodão, avaliando sua eficácia na promoção da rastreabilidade, confiança e verificabilidade, bem como seu potencial para resolver desafios específicos relacionados à transparência e segurança nesse setor.

Para que o objetivo geral seja atingido, os seguintes objetivos específicos serão abordados:

- Realizar uma revisão bibliográfica detalhada sobre o SSI.
- Analisar criticamente os principais desafios enfrentados atualmente na cadeia produtiva do algodão em termos de rastreabilidade, confiança e verificabilidade.
- Propor e desenvolver um projeto de arquitetura e sistema descentralizado, rastreável, confiável e verificável, utilizando SSI na cadeia produtiva do algodão.
- Realizar uma prova de conceito, envolvendo a aplicação do SSI em um segmento específico da cadeia produtiva do algodão que envolve a produção e comercialização de fardinhos de algodão.

- Avaliar a eficácia do SSI na garantia da rastreabilidade, confiança e verificabilidade na cadeia produtiva do algodão, comparando os resultados obtidos com as práticas convencionais.
- Identificar desafios e possíveis melhorias para a adoção e escalabilidade do SSI na cadeia produtiva do algodão, propondo recomendações e diretrizes para sua implementação bem-sucedida.

## 1.2 ESTRUTURA DO TEXTO

Este trabalho está organizado em 6 capítulos. No Capítulo 2 é apresentada a revisão da literatura com o conceito de Identidade Digital Autossoberana, a descrição de sua arquitetura e o fluxo de comunicação entre seus elementos. No Capítulo 3 são apresentados: a cadeia produtiva do algodão e os trabalhos relacionados, cujo mapeamento buscou identificar a existência de trabalhos similares que abordassem as áreas foco deste trabalho: cadeia produtiva ou de *supply chain*, rastreabilidade ou confiabilidade, SSI e algodão, com o objetivo de analisar tendências de publicação nessas áreas. No Capítulo 4 encontra-se a proposta deste trabalho, fornecendo uma análise detalhada de seus componentes, arquitetura e funcionamento. Este capítulo oferece uma visão abrangente do sistema, destacando sua estrutura e operação. No Capítulo 5 é possível entender o ambiente de testes, a descrição dos experimentos e os resultados obtidos. O Capítulo 6 encerra o texto com as considerações finais e com as descrições de possíveis pontos a serem explorados em trabalhos futuros.

## 2 IDENTIDADE DIGITAL AUTOSSOBERANA

Também conhecida como identidade auto gerenciada e identidade controlada pelo usuário, a *Self-Sovereign Identity* (SSI) é um modelo de gerenciamento de identidade no qual o titular tem controle total sobre seus dados e decide como e sob quais condições estes devem ser compartilhados com outras pessoas (SOLTANI; NGUYEN; AN, 2021).

Čučko e Turkanović (2021) estabelecem que o SSI é uma abordagem de identidade emergente e descentralizada que permite que entidades como indivíduos, organizações e objetos, controlem totalmente sua identidade digital sem depender de qualquer autoridade externa, eliminando um único ponto de falha (ČUČKO; TURKANOVÍČ, 2021).

Em seu artigo "*The Path to Self-Sovereign Identity*" (ALLEN, 2016), Christopher Allen define SSI da seguinte forma:

“...O usuário deve centralizar a administração da identidade. Isso requer não apenas a interoperabilidade da identidade de um usuário em vários locais, com o consentimento do usuário, mas também o verdadeiro controle do usuário dessa identidade digital, criando sua autonomia. Para conseguir isso, uma identidade autossobrerana deve ser transportável; ela não pode ser restrita a um site ou localidade. Uma identidade autossobrerana também deve permitir que usuários comuns façam declarações, que podem incluir informações de identificação pessoal ou fatos sobre capacidade pessoal ou associação de grupo. Pode até conter informações sobre o usuário que foram afirmadas por outras pessoas ou grupos.”

Nesse mesmo artigo, Allen (2016) fornece dez princípios que definem um sistema SSI (ALLEN, 2016). Esses princípios estão completamente alinhados com as 7 Leis da Identidade de Kim Cameron. São estes:

1. Existência: Usuários devem existir de forma independente. Um usuário deve ter a capacidade de existir no mundo digital, sem a necessidade de um terceiro, *i.e.*, a existência ou não de outras entidades é irrelevante para sua identidade existir.
2. Controle: Usuários devem controlar suas identidades. Um usuário deve ter a liberdade de gerenciar seus atributos da forma desejada pois têm autoridade sobre seus dados de identidade. Em suma, ele decide o que faz com sua identi-

dade, *e.g.*, outros podem endossar o João, dizendo que ele realmente é o João, mas só o João controla o que faz com essa informação.

3. **Acesso:** Usuários devem ter acesso aos seus próprios dados. Nenhuma entidade deve armazenar dados sobre o usuário sem que ele saiba e tenha acesso.
4. **Transparência:** Sistemas e algoritmos devem ser transparentes. Sistemas e algoritmos devem ser simples e os mecanismos que estabelecem identidades devem ser abertos.
5. **Persistência:** As identidades devem ter vida longa. Uma identidade deve durar até quando o usuário quiser. A formação da identidade é um processo contínuo e cada sistema de gerenciamento de identidade deve ser projetado para ser suficientemente flexível para permitir aos titulares obter, modificar ou remover seus dados de identidade.
6. **Portabilidade:** Informações e serviços sobre identidade devem ser portáveis. O titular da identidade deve ter a capacidade de transportar seus dados de identidade de um local para outro. Esse processo é fundamental para a longevidade dos dados de identidade.
7. **Interoperabilidade:** As identidades são de pouco valor se funcionarem apenas em nichos limitados e, portanto, devem ser usadas o mais amplamente possível.
8. **Consentimento:** Os usuários devem concordar com o uso de sua identidade, *i.e.*, o compartilhamento de dados pessoais pode ser feito apenas com o consentimento do usuário.
9. **Minimização:** A divulgação de dados proprietários deve ser minimizada. Exemplificando, se a idade mínima de um usuário for exigida para acessar uma página, ele não deverá fornecer o dia, mês e ano de seu nascimento. Em vez disso, a divulgação do usuário deve ser minimizada fornecendo apenas o requisito mínimo, *i.e.*, os anos de idade.
10. **Proteção:** Os direitos dos usuários devem ser respeitados. Um sistema de identidade autossobrano deve garantir proteção aos usuários dentro da rede, de acordo com os regulamentos sobre direitos digitais como a Lei Geral de Proteção de Dados e o *General Data Protection Regulation*.

Esses dez princípios constituem um catálogo abrangente de requisitos essenciais para a implementação de uma solução SSI. No entanto, para uma compreensão completa e efetiva, é preciso explorar não apenas os requisitos, mas também as nuances técnicas envolvidas na implementação dessa solução.

## 2.1 ARQUITETURA

*Self-Sovereign Identities* oferece uma nova perspectiva sobre um dos desafios mais importantes da sociedade e da computação: gerenciar com segurança as identidades digitais (PREUKSCHAT; REED, 2021). Conceitualmente, ela é um conjunto de princípios sobre como o controle de identidade e dados pessoais deve funcionar nas redes digitais. E, em nível estrutural, é um conjunto de tecnologias que se baseiam em conceitos centrais de gerenciamento de identidade, sistemas distribuídos e criptografia.

Em muitos casos, esses conceitos centrais estão estabelecidos há décadas, porém, a inovação é a forma como eles são reunidos para criar esse novo modelo de gerenciamento de identidade digital (PREUKSCHAT; REED, 2021). Os sete blocos de construção que formam a base de uma arquitetura SSI são as credenciais verificáveis, o triângulo da confiança, os identificadores descentralizados, as carteiras e agentes digitais, os registros de dados verificáveis e as estruturas de governança, devidamente detalhados nas subseções a seguir.

### 2.1.1 Credenciais Verificáveis

Uma credencial é um conjunto de afirmações que uma autoridade declara ser verdadeira sobre o sujeito, também chamado de assunto da credencial, e que, por sua vez, permite que este convença os outros (que confiam nessa autoridade) dessas verdades, *e.g.*, uma certidão de nascimento emitida por um hospital ou cartório que comprova a data, o local de nascimento e a filiação; um diploma emitido por uma universidade que comprova a conclusão do nível superior; um passaporte emitido pelo governo de um país que prova a cidadania (SPORNY; LONGLEY; CHADWICK, 2022; SIQUEIRA; CONCEIÇÃO; ROCHA, ; PREUKSCHAT; REED, 2021).

Todos esses exemplos são de credenciais sobre um assunto humano, porém, as credenciais verificáveis não se limitam aos humanos, *e.g.*, um veterinário pode emitir um credencial verificável sobre vacinas para um animal de estimação ou um fabricante pode emitir credenciais sobre um dispositivo de IoT (PREUKSCHAT; REED, 2021).

Dentre as afirmações que uma credencial pode declarar sobre o assunto estão informações relacionadas aos seus atributos (como nome, idade, altura, peso), seus relacionamentos (como mãe, pai, empregador) e seus agentes (quem o representa, *e.g.*, procurador, dispositivo pessoal) (MARINO et al., 2019). E ainda, para se qualificar como uma credencial, as afirmações devem ser verificáveis de alguma forma. Isso significa dizer que deve ser possível determinar quem emitiu a credencial, que não foi adulterada desde que foi emitida, e que não expirou ou foi revogada (PREUKSCHAT;

REED, 2021).

Como ilustrado na Figura 1, as entidades e funções envolvidas no ecossistema das credenciais verificáveis são as seguintes (SPORNY; LONGLEY; CHADWICK, 2022; PREUKSCHAT; REED, 2021):

- **Emissor:** entidade que afirma fatos sobre um assunto, emitindo credenciais verificáveis para o mesmo.
- **Assunto:** entidade cujas informações são armazenadas na credencial verificável. Um assunto pode ser qualquer coisa: uma pessoa, organização, coisa feita pelo homem, coisa natural, coisa lógica e assim por diante.
- **Titular:** entidade que detém as credenciais verificáveis e as usa para apresentar provas sobre uma afirmação. Na maioria dos casos, o titular é o assunto da credencial, mas em alguns casos pode não ser, *e.g.*, se o assunto for um gato de estimação e a credencial verificável for um certificado de vacinação, o emissor emitirá a credencial com as informações do gato, que é o assunto, e a enviará para o dono do gato, que será o titular.
- **Verificador:** entidade que verifica as afirmações feitas pelo titular, através da validação das credenciais verificáveis apresentadas.
- **Carteira Digital:** software que armazena as credenciais verificáveis do titular. Em muitos casos, a carteira pode ser parte integrante do agente digital do titular.
- **Agente Digital:** software que interage com o ecossistema das credenciais verificáveis em nome do titular.
- **Registro de Dados Verificável:** repositório de informações, aberto e descentralizado, que contém todos os dados e metadados (esquemas de credenciais) que permitem o funcionamento do ecossistema das credenciais verificáveis.

Esse ecossistema composto por emissores, verificadores, titulares, carteiras e agentes digitais e o registro de dados verificável, trabalha em conjunto em uma rede de confiança, cujo arranjo típico pode operar da seguinte forma (PREUKSCHAT; REED, 2021):

1. Um verificador define suas políticas para aceitar credenciais verificáveis de titulares, para que seja possível eles utilizarem seus serviços. Cada serviço ofertado pelo verificador pode ter uma política diferente e, cada política diz em quais emissores o verificador confia para emitir credenciais verificáveis para este serviço, *e.g.*, um site de uma pizzaria pode ter uma política que diz que, para fazer um

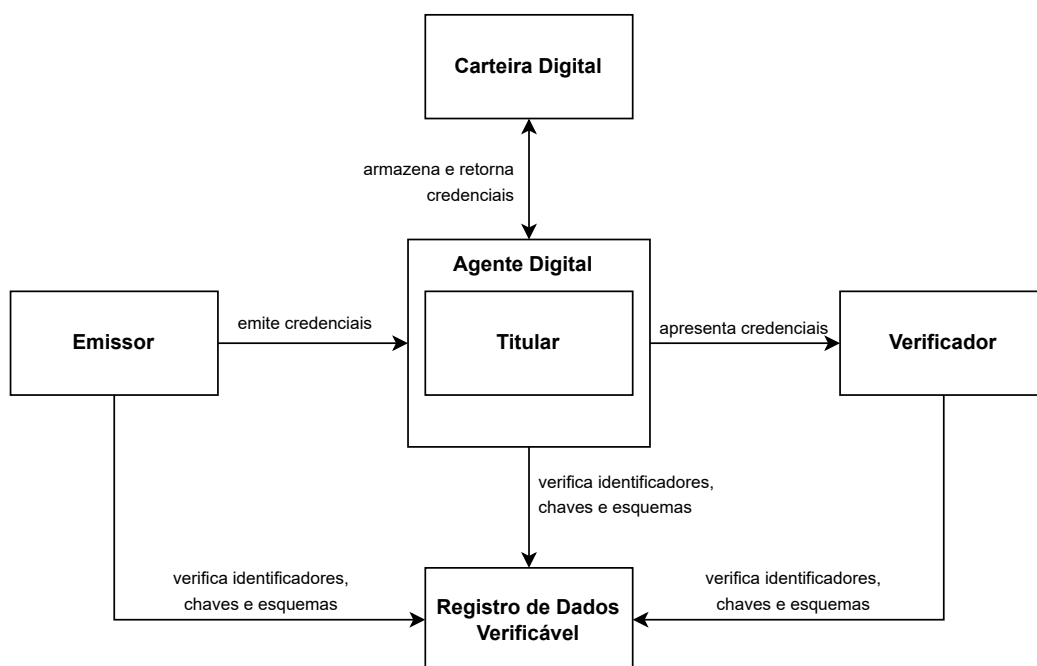


Figura 1 – Ecosistema das Credenciais Verificáveis

Fonte: (PREUKSCHAT; REED, 2021)

pedido online de uma pizza, o usuário deve apresentar uma credencial verificável de um cartão de crédito emitido pela Visa ou Mastercard, para o pagamento.

2. A qualquer momento, os emissores emitem credenciais verificáveis para os titulares, que as armazenam em suas carteiras digitais.
3. O titular solicita um determinado serviço de um verificador.
4. O verificador devolve sua política de aceite de credenciais (definida no passo 1) ao agente do titular, que verifica se este possui o conjunto necessário de credenciais verificáveis em sua carteira, para satisfazer a política.
5. O titular apresenta o conjunto de credenciais verificáveis ao verificador.
6. O verificador verifica que as credenciais verificáveis apresentadas possuem assinaturas digitais autênticas, satisfazem a sua política, e são efetivamente de posse do titular.
7. Se todas as condições estiverem satisfeitas, o verificador realiza o serviço solicitado pelo titular.

O *World Wide Web Consortium (W3C)*, organização internacional de padrões que desenvolve os pilares de tecnologias Web, através de um grupo de trabalho, produziu a recomendação "Modelo de dados de credenciais verificáveis v1.1"(SPORNY;

LONGLEY; CHADWICK, 2022) que especifica e promove a implementação para uso geral das credenciais verificáveis. Tecnicamente, essa recomendação define o modelo de dados para credenciais verificáveis que um emissor fornece a um titular, e o modelo de dados para as apresentações verificáveis que um titular pode apresentar a um verificador.

Segundo a recomendação do W3C, o modelo de dados para credenciais verificáveis que um emissor fornece a um titular, precisa conter basicamente três blocos de informações: metadados, afirmações e prova, no formato JSON, conforme Figura 2(a) (SPORNY; LONGLEY; CHADWICK, 2022).

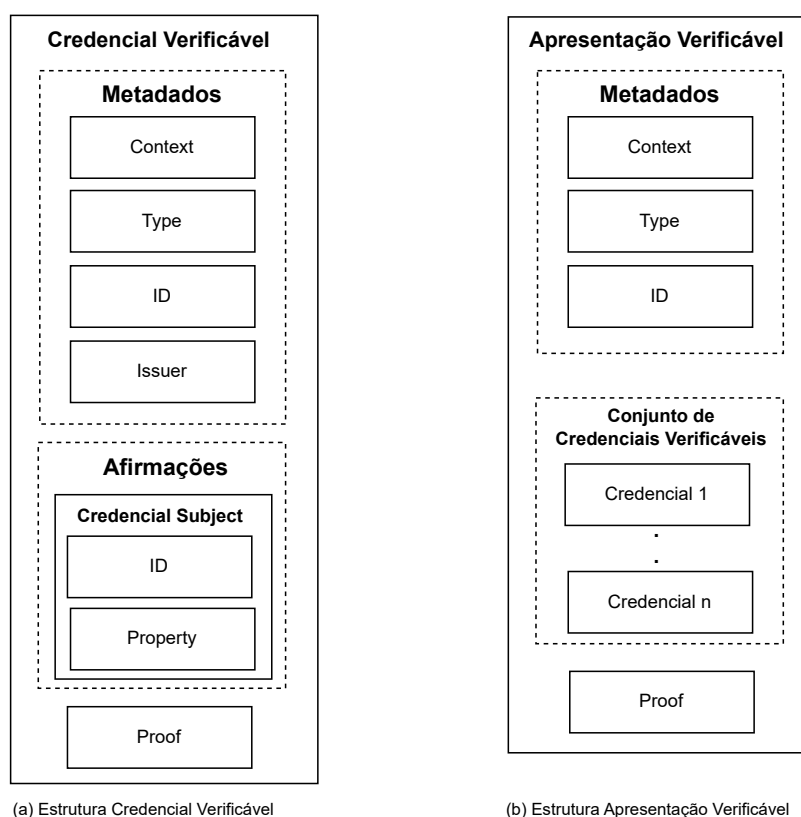


Figura 2 – Propriedades das Credenciais e Apresentações Verificáveis

Fonte: (PREUKSCHAT; REED, 2021)

As apresentações verificáveis, por sua vez, são pacotes de evidências construídos pelos titulares para satisfazer os requisitos de um verificador. Segundo a recomendação do W3C, o modelo de dados para as apresentações verificáveis que um titular pode apresentar a um verificador, possui estrutura semelhante a uma credencial, contendo os blocos: metadados, conjunto de afirmações e prova, conforme Figura 2(b) (SPORNY; LONGLEY; CHADWICK, 2022).

As credenciais verificáveis permitem que esse pacote de evidências seja gerado possibilitando que os titulares escolham afirmações de diversas credenciais, pro-

venientes de diferentes emissores, formando uma apresentação verificável que contém somente os atributos requeridos pelo verificador, sem que os demais sejam expostos (LÓPEZ, 2020). Essa característica é descrita como divulgação seletiva e confere às identidades digitais autossobranas aspectos de privacidade ao preservar a confidencialidade de atributos individuais e, ao mesmo tempo, reduzir o risco do verificador manusear dados sensíveis (PREUKSCHAT; REED, 2021).

A ferramenta criptográfica que possibilita a divulgação seletiva das credenciais verificáveis é conhecida como *Zero-Knowledge Proof* (ZKP). Uma ZKP refere-se a uma classe de algoritmos ou protocolos criptográficos pelo qual uma parte (o titular) pode provar à outra parte (o verificador) que uma determinada afirmação é verdadeira, sem transmitir qualquer informação além do fato de que a afirmação é realmente verdadeira (GOLDREICH; MICALI; WIGDERSON, 1991), *e.g.*, provar ser maior de idade sem ter que informar a data de nascimento ou outros dados como nome, foto, RG e CPF.

### 2.1.2 Triângulo da Confiança

O triângulo da confiança é formado pelo **emissor**, pelo **titular** e pelo **verificador** das credenciais. A relação entre emissores, titulares e verificadores é referida como o triângulo de confiança porque é, fundamentalmente, como as relações de confiança humana são transmitidas através de uma rede digital (DAVIE et al., 2019).

A Figura 3 ilustra como as credenciais verificáveis só transmitem confiança se o verificador confiar no emissor. Isso não significa que o verificador deve ter uma relação direta ou jurídica com o emissor, mas sim que o verificador está disposto a tomar uma decisão de negócios (“Aceito este cartão de crédito?” “Aceito embarcar este passageiro?” “Vou admitir este aluno?”) com base no nível de confiança que ele tem no emissor (PREUKSCHAT; REED, 2021).

### 2.1.3 *Decentralized Identifiers* (DIDs)

Diariamente identificadores são utilizados em uma ampla variedade de contextos, seja como endereços de comunicação (números de telefone, endereços de e-mail, nomes de usuário), números de identificação (para passaportes, carteiras de motorista, carteiras de identidade, CPF), identificadores de produtos (números de série, códigos de barras, RFIDs), bem como para identificar recursos e páginas na Internet (URI, URL) (SPORNY et al., 2021; PREUKSCHAT; REED, 2021). Nesse universo, os DIDs são um novo tipo de identificadores globalmente exclusivos, projetados para permitir que entidades gerem seus próprios identificadores usando sistemas nos quais confiam, e comprovem o controle sobre eles usando provas criptográficas (PREUKSCHAT; REED, 2021).

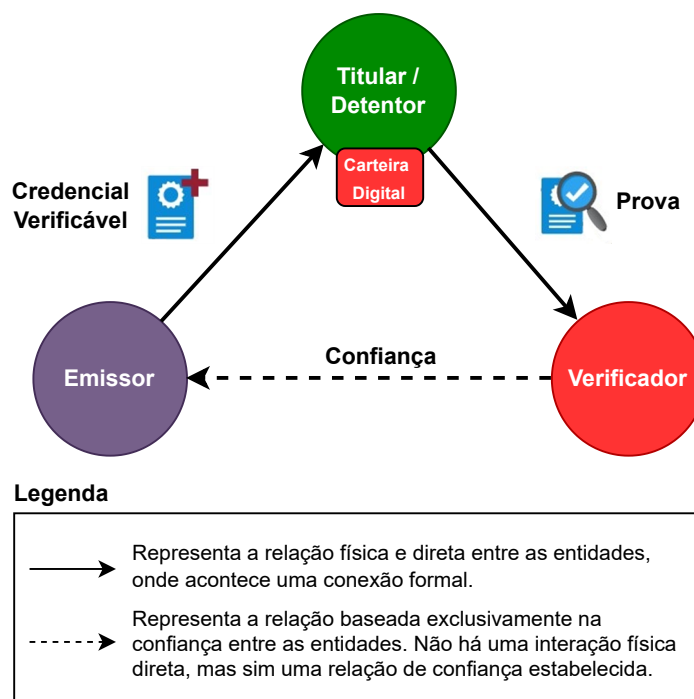


Figura 3 – Triângulo da Confiança no SSI

Fonte: (DAVIE et al., 2019)

Como a geração dos DIDs é controlada pela entidade, cada qual pode ter quantos DIDs forem necessários para manter a separação desejada de identidades. O uso desses identificadores também fornece um meio universal de identificação de recursos, criptograficamente verificável, que não precisa confiar em quaisquer autoridades centralizadas e também garante sua existência contínua (SPORNY; LONGLEY; CHADWICK, 2022).

Assim como para as credenciais verificáveis, o W3C, através de um grupo de trabalho, produziu a recomendação 'Identificadores descentralizados (DIDs) v1.0' (SPORNY et al., 2021) que especifica a arquitetura principal, modelo de dados e representação para uso dos DIDs. Segundo essa recomendação, estruturalmente, um DID é uma sequência de texto simples que consiste em três partes: 1) identificador do esquema DID, 2) identificador para o método DID e 3) identificador específico do método DID (Figura 4). O identificador do esquema DID define a estrutura do identificador descentralizado; o método DID define como ele deve ser implementado, e o identificador específico do método determina como esse DID é criado, resolvido, atualizado ou desativado.

Cada DID tem exatamente um documento DID associado, contendo metadados sobre o assunto DID, que é o dono desse identificador. Um documento DID é um conjunto de dados relacionados ao assunto DID e os seus métodos, projetado para ser consumido por aplicativos ou serviços de identidade digital, os quais usam DIDs



Figura 4 – Formato geral de um DID

Fonte: (SPORNY et al., 2021)

como blocos de construção fundamentais (Figura 5) (PREUKSCHAT; REED, 2021). A entidade que controla o DID e seu documento DID é chamada de controlador DID. Em muitos casos, o controlador DID é o mesmo que o assunto DID, mas também podem ser entidades diferentes.

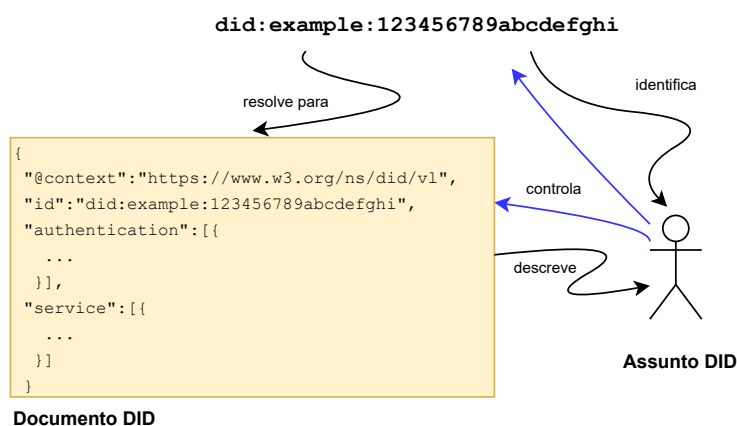


Figura 5 – Relacionamento entre DID, Documento DID e Assunto DID

Fonte: (PREUKSCHAT; REED, 2021)

Existem diferentes tipos de DIDs na comunidade SSI e todos suportam a mesma funcionalidade básica, mas diferem em como essa funcionalidade é implementada, *e.g.*, como exatamente um DID é criado, ou onde e como o documento DID é armazenado e recuperado (PREUKSCHAT; REED, 2021). Esses diferentes tipos de DIDs são conhecidos como métodos DID. Os métodos DID também podem diferir em fatores como escalabilidade, desempenho ou custo de infraestrutura técnica subjacente. Uma consequência dessa variedade tecnológica é que alguns podem ser mais adequados para certos casos de uso do que outros.

Por fim, o processo de obtenção do documento DID associado a um DID é chamado de resolvidor DID, e permite que aplicativos e serviços habilitados para DID descubram os metadados sobre o assunto DID, expresso pelo documento DID. Esses

metadados são usados para interação com o assunto DID. O processo de resolução é baseado na operação de leitura definida pelo método DID, que pode variar dependendo de como ele é projetado. Isso significa que a resolução DID não está restrita à um único protocolo, mas sim, deve ser considerada uma função abstrata, ou um algoritmo que recebe um DID como entrada e retorna o documento DID como resultado.

#### **2.1.4 Carteiras e Agentes Digitais**

Uma carteira digital consiste em um software que permite que o controlador da carteira gere, armazene, gerencie e proteja chaves criptográficas, segredos e outros dados privados confidenciais (PREUKSCHAT; REED, 2021). As implementações de carteira digital para o ecossistema SSI armazenam os DIDs, chaves criptográficas e credenciais verificáveis do titular.

O agente digital é o software que permite que uma entidade execute ações, realize comunicações, armazene informações e rastreie o uso da carteira digital. Dessa forma, asseguram a comunicação entre os emissores, titulares e verificadores, e atuam como guardiões da carteira digital garantindo que apenas o responsável pelas credenciais verificáveis e chaves criptográficas contidas nela, possa usá-las (MARINO et al., 2019; PREUKSCHAT; REED, 2021).

Existem duas categorias de agentes com base em sua localização: os agentes de borda que operam na borda da rede, *e.g.*, nos dispositivos locais de um titular de identidade, e os agentes de nuvem que operam na nuvem, hospedados por provedores de serviços de nuvem. Todo o objetivo do agente digital é construir e manter relacionamentos de confiança digital em nome de seu controlador. Embora implementações específicas de carteiras e agentes possam diferir na maneira como dividem essas funções, em termos gerais, elas cobrirão as áreas da Tabela 1.

#### **2.1.5 Registro de Dados Verificável**

Um registro de dados verificável, no SSI, tem a função de mediar a criação e verificação de dados necessários ao uso das credenciais verificáveis, *e.g.*, identificadores descentralizados e chaves públicas. Exemplos de registros de dados verificáveis incluem bancos de dados confiáveis, bancos de dados descentralizados, bancos de dados de identificação do governo e livros-razão distribuídos (SPORNY; LONGLEY; CHADWICK, 2022).

#### **2.1.6 Estruturas de Governança**

As estruturas de governança são administradas por uma entidade chamada de autoridade de governança e, criam o segundo triângulo de confiança, apresentado

Tabela 1 – Funções Principais das Carteiras e Agentes Digitais

Componente	Função
<b>Agente</b>	Mensagens — um agente funciona como um aplicativo de e-mail, <i>i.e.</i> , envia e recebe dados, mensagens estruturadas e notificações em nome do controlador.
	Roteamento — alguns agentes servem como intermediários para rotear mensagens de agente para agente.
	Backup e recuperação — dado o valor e a sensibilidade dos dados armazenados em uma carteira digital, o agente deve oferecer suporte a opções de backup e recuperação em caso de perda, corrupção ou invasão dos dados.
	Armazenamento seguro — este componente de um agente chama os serviços da carteira, normalmente por meio de uma API segura fornecida pela carteira.
<b>Carteira</b>	Sistema de gerenciamento de chaves — determina como a carteira digital trata a geração, rotação, revogação, armazenamento, assinatura e proteção de chaves criptográficas.
	Armazenamento criptografado — estabelece suporte ao armazenamento protegido das chaves, segredos e outros dados privados que o controlador decide armazenar na carteira.

Fonte: (PREUKSCHAT; REED, 2021)

na metade inferior da Figura 6 (PREUKSCHAT; REED, 2021).

Os *frameworks* de governança especificam as políticas e procedimentos que os emissores devem seguir para emitir uma credencial. Em alguns casos, eles também especificam os termos e condições com os quais os titulares devem concordar para obter credenciais, ou com os quais os verificadores devem concordar ao verificar as credenciais.

## 2.2 RESUMINDO OS BLOCOS DE CONSTRUÇÃO E DEFININDO A PILHA SSI

A Tabela 2 sumariza a função de cada bloco que compõe a arquitetura do SSI. Esse conjunto de blocos se une para construir uma imagem geral, seguindo um modelo de arquitetura de quatro camadas para infraestrutura de confiança digital alimentada por SSI, chamada pilha SSI (Figura 7). A pilha SSI descreve as dependências arquiteturais fundamentais no SSI, sendo as duas camadas inferiores destinadas a alcançar a confiança técnica do modelo, e as duas camadas superiores destinadas a alcançar a confiança humana.

A **Camada 1** é a parte inferior da pilha, cujas chaves públicas e identificadores descentralizados (DIDs) são definidos e gerenciados. Essa camada precisa garantir que todas as partes interessadas concordem com a mesma verdade sobre o que, ou quem, um identificador referencia, e como o controle desse identificador pode ser comprovado usando chaves criptográficas. Também deve permitir que todas as partes leiam e gravem dados sem depender da interferência de autoridades centrais.

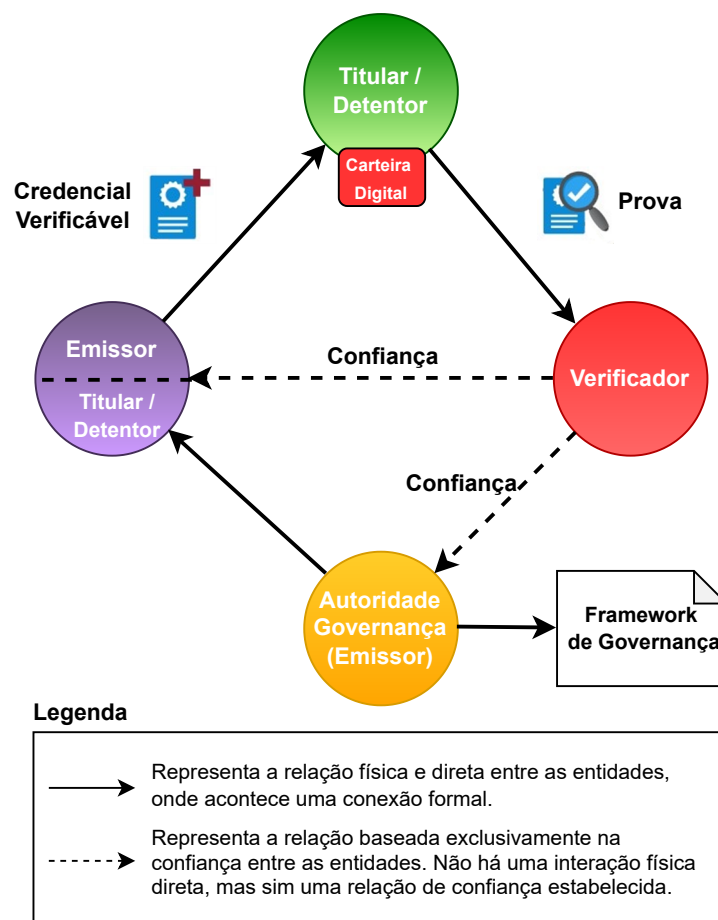


Figura 6 – Segundo Triângulo da Confiança do SSI

Fonte: (DAVIE et al., 2019)

Uma das maneiras de dispor desses recursos é utilizar tecnologias como blockchain, *Distributed Ledger Technology* (DLT), gráficos acíclicos direcionados distribuídos (e.g. IOTA) ou tabelas hash distribuídas (e.g. IPFS) (PREUKSCHAT; REED, 2021). Especificamente sobre blockchain, a partir de 2016, blockchains destinados à SSI começaram a ser construídos, com tipos de transações e registros que facilitam o gerenciamento dos DIDs e suportam a *Zero-Knowledge Proof*. No entanto, a utilização desses recursos na Camada 1 se limita a armazenar: (TOBIN, 2017)

- Definições de esquemas de credenciais verificáveis, permitindo a interoperabilidade semântica.
- Registros de revogação de credenciais.
- DIDs e *endpoints* de agentes digitais.

Além da blockchain, existem outras possibilidades para a Camada 1, como o uso do método DID *peer-to-peer* (SPORNY et al., 2022), que são DIDs gerados diretamente nas carteiras digitais das partes envolvidas, e trocados usando seus agentes

Tabela 2 – Blocos de construção do SSI

<b>Credenciais Verificáveis</b>	Equivalente digital das credenciais físicas que carregamos em nossas carteiras para provar algum aspecto de nossas identidades
<b>Triângulo da Confiança (Emissor, Titular e Verificador)</b>	São os três papéis do triângulo de confiança que fazem as credenciais funcionarem: emitir a credencial, guardá-la em uma carteira e verificá-la quando o titular a apresentar.
<b>Identificadores Descentralizados (DIDs)</b>	Novo tipo de endereço digital alimentado por criptografia que não exigem uma autoridade de registro centralizada.
<b>Carteiras e Agentes Digitais</b>	As carteiras digitais são o equivalente digital de nossas carteiras físicas, cuja função é armazenar as credenciais verificáveis. Os agentes são os softwares que permitem usar as carteiras digitais para obter e apresentar credenciais, gerenciar conexões e trocar credenciais verificáveis com segurança.
<b>Registros de Dados Verificáveis</b>	Bancos de dados distribuídos e protegidos criptograficamente que podem servir como fonte de verdade para DIDs e chaves públicas sem estarem sujeitos a pontos únicos de falha ou ataque.
<b>Estruturas de Governança</b>	Conjunto de regras comerciais, legais e técnicas para usar a infraestrutura SSI que permitirá ecossistemas de confiança digital interoperáveis de qualquer tamanho e escala.

Fonte: (STRÜKER et al., 2021; PREUKSCHAT; REED, 2021)

digitais. Recibos com assinatura tripla (GRIGG, 2005) é outro protocolo que também resolve esse problema sem qualquer blockchain. Nesse protocolo, cada parte assina uma descrição da transação que inclui não apenas as entradas, mas também as saídas (saldo resultante). Um auditor externo também assina. Uma vez que todas as três assinaturas se acumulam, não há dúvida sobre a veracidade de uma transação – e como os dados assinados incluem o saldo resultante além das entradas, nenhuma transação anterior precisa ser consultada para saber o efeito da transação. Por fim, Infraestrutura de Recebimento de Eventos Chave (KERI) (SMITH, 2019) é outra opção, sendo uma arquitetura completa para DIDs portáteis desenvolvida em torno do conceito de identificadores autocertificados.

A **Camada 2** trata do estabelecimento de comunicações confiáveis entre as partes. É a camada dos agentes digitais, carteiras e armazenamentos de dados criptografados, cuja arquitetura se divide em duas categorias principais: protocolo e interface. As principais arquiteturas de protocolo são: o projeto de protocolo baseado na Web, que segue os mesmos padrões básicos de protocolo HTTP, com uma dependência do padrão *Transport Layer Security* (TLS) usado no protocolo HTTPS; e o projeto de protocolo baseado em mensagem que usa o protocolo *DIDComm Messaging* (DIF, 2022a) para comunicações entre agentes digitais.

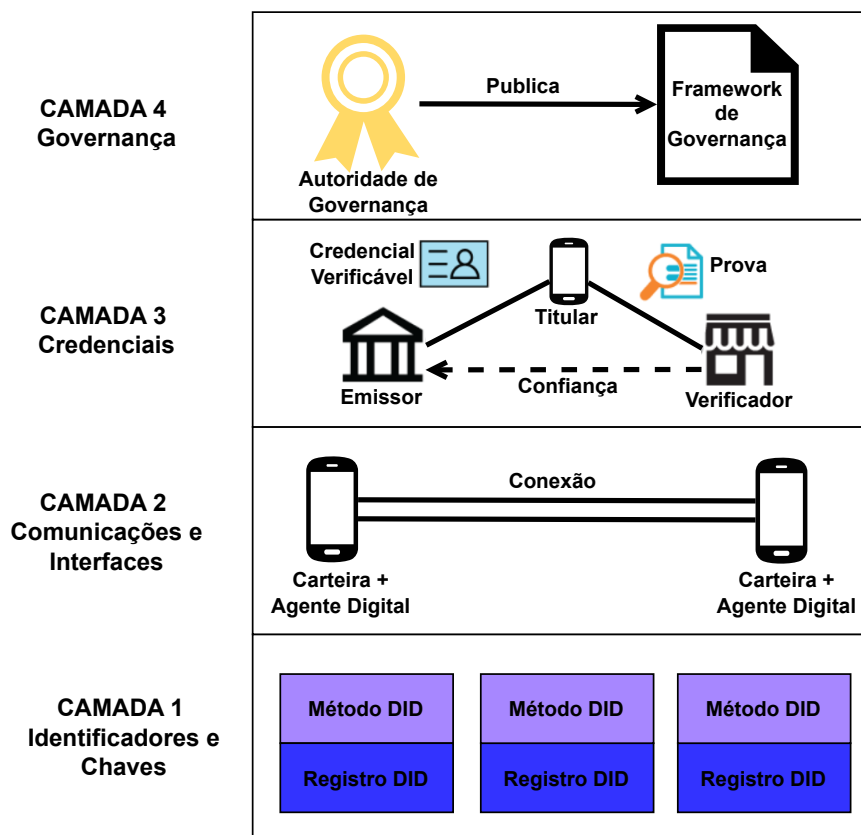


Figura 7 – Pilha SSI

Fonte: (PREUKSCHAT; REED, 2021)

Já os projetos de *design* de interface englobam: o *design* de interface orientado a API que favorece o uso de aplicativos descentralizados da web (Dapps); o *design* de interface orientado a dados que utiliza armazenamentos de dados criptografados para descobrir, compartilhar e gerenciar o acesso a dados de identidade (DIF, 2022b); e o *design* de interface orientado a mensagens que usa agentes digitais que roteiam as mensagens e interações que compartilham.

Especificamente, a **Camada 3** é a camada do triângulo da confiança, cujo objetivo é oferecer suporte para as credenciais verificáveis interoperáveis que podem ser usadas – de qualquer emissor, para qualquer titular, para qualquer verificador. Essa camada descreve as opções de formato das credenciais verificáveis e os protocolos usados para trocá-las. A necessidade de um padrão mundial para interoperabilidade de credenciais verificáveis deu origem a recomendação do W3C, estabelecendo um modelo de dados de credenciais verificáveis já detalhado anteriormente.

Por fim, a **Camada 4** diz respeito às estruturas de governança que existem para descrever as políticas, procedimentos e mecanismos para a operação da confiança digital na comunidade SSI.

## 2.3 PROTOCOLOS DE COMUNICAÇÃO

Para permitir o estabelecimento de uma comunicação entre as diferentes entidades é necessário estabelecer protocolos de comunicação, de modo que todos os agentes digitais sejam capazes de se entenderem mutuamente. Ao longo desta Seção serão abordados os três principais protocolos de comunicação entre agentes SSI: (1) Protocolo de conexão; (2) Protocolo de emissão da credencial; (3) Protocolo de apresentação verificável (provas) (PREUKSCHAT; REED, 2021). Estes três protocolos representam o núcleo de todas as interações entre entidades e são indispensáveis a qualquer agente digital.

### 2.3.1 Protocolo de Conexão

Antes de trocarem informações sobre credenciais e atributos, as entidades precisam estabelecer uma comunicação segura entre elas. O protocolo de conexão define os passos para o estabelecimento de uma comunicação segura (WEST et al., 2019) de modo que os agentes consigam interagir entre si.

Neste protocolo existem dois papéis: *inviter* e *invitee*. O *inviter* é a entidade que inicia o protocolo através da criação de um convite de conexão. O *invitee* é a entidade que vê e aceita o convite, através do envio de um pedido de conexão à entidade que o publicou. A Figura 8, por meio de um diagrama de fluxo, mostra o processo de estabelecimento de uma conexão, desde a criação do convite até a ativação de uma conexão.

O protocolo inicia com o *inviter* compartilhando um convite de conexão (utilizando um objeto JSON, QRCode, URL, entre outros) que contém informações sobre como entrar em contato com ela. Todos os convites possuem um DID público associado, cujo documento pode ser obtido consultando o Registro de Dados Verificável (RDV). Este documento contém todas as informações adicionais necessárias para contatar o dono deste DID, como a chave pública e o seu *endpoint* de comunicação.

Se um *invitee* pretender estabelecer uma conexão com o *inviter*, deve enviar uma mensagem de pedido de conexão, cifrando esta mensagem com a chave pública presente no documento do DID. Neste pedido de conexão, o *invitee* deve enviar o documento referente ao DID, de modo que o *inviter* tenha acesso ao *endpoint* de comunicação do agente do mesmo.

Ao receber o pedido de conexão, o *inviter* processa o documento recebido e obtém as informações sobre como contatar o *invitee* (chaves públicas, *endpoint* de comunicação, entre outros). De posse dessas informações, envia ao *invitee* uma mensagem de resposta, cifrando-a com a chave pública presente no documento que recebeu. O campo que contém a informação sobre o DID e o documento associado

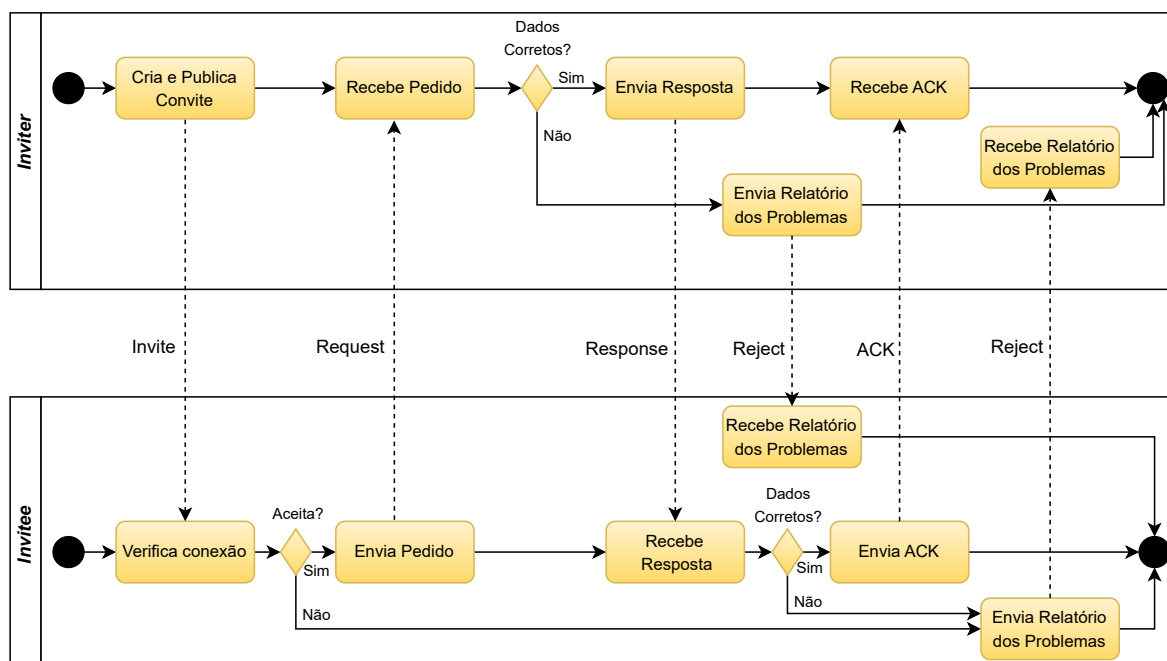


Figura 8 – Protocolo de conexão

Fonte: (PEIXOTO, 2021)

deve ser assinado pelo *inviter* com a chave privada associada ao convite, de forma a autenticar estas informações.

Ao receber a resposta de conexão, o *invitee* verifica a assinatura efetuada sobre o documento do DID, recorrendo à chave pública contida no convite inicial, de forma a comprovar que foi o *inviter* quem lhe enviou esse documento. Se a verificação for bem sucedida, o *invitee* armazena o documento que recebeu na sua carteira digital e envia uma mensagem de confirmação, designada por *connection acknowledgement*, utilizando para tal o sub-protocolo ACKs (HARDMAN, 2021). Após a conexão se estabelecer, as duas entidades podem comunicar-se entre si de forma segura, recorrendo às chaves públicas contidas nos respectivos documentos recebidos para cifrar todas as mensagens.

### 2.3.2 Protocolo de emissão da credencial

A emissão de credenciais envolve duas entidades: o Emissor e o Titular. Para que o Emissor emita uma credencial é necessário que ambas as partes estejam de acordo quanto ao tipo de informações que essa credencial deverá conter. O protocolo de emissão da credencial (KHATEEV, 2019a) especifica as mensagens trocadas, desde o processo inicial de negociação, até a mensagem de confirmação enviada pelo Titular confirmando que a credencial foi recebida. A Figura 9 representa o processo de emissão de credenciais por meio de um diagrama de fluxo.

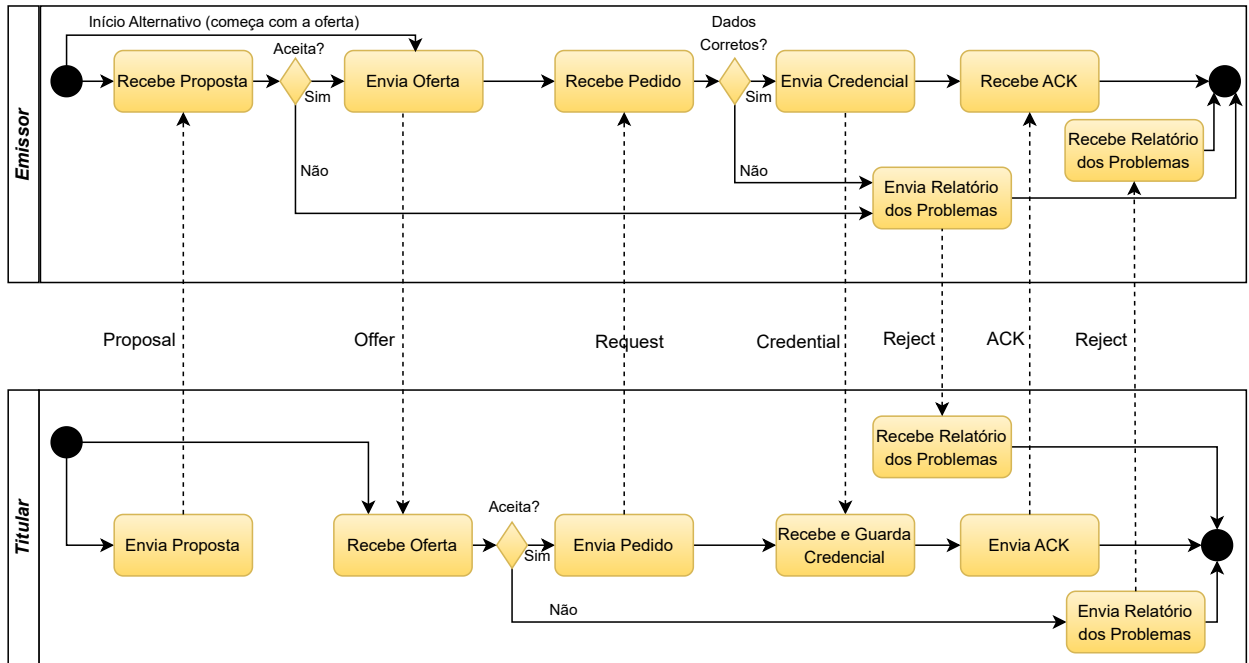


Figura 9 – Protocolo de emissão da credencial

Fonte: (PEIXOTO, 2021)

Este protocolo apresenta dois inícios alternativos. Na primeira alternativa o Titular inicia o protocolo por meio do envio de uma proposta ao Emissor, na qual indica qual esquema de dados pretende usar, e qual valor cada um dos atributos desse esquema deve possuir. Já a segunda alternativa exclui a fase inicial de envio e recepção de uma proposta, sendo que o Emissor inicia o protocolo através da oferta de uma credencial. Esta oferta deve conter a definição da credencial que o Emissor pretende usar para emitir a credencial e uma pré-visualização dos atributos que irão ser incluídos na credencial com seus respectivos valores.

Ao receber a oferta, o Titular verifica se todos os atributos apresentados estão corretos. Se encontrar algum problema deverá cancelar o processo e notificar o Emissor, indicando a razão do cancelamento. Caso tudo esteja correto, o Titular continua o processo por meio do envio de um pedido que contém a definição da credencial que deverá ser usada pelo Emissor para a emissão da credencial, bem como um *master secret*, que o Emissor deverá incorporar na credencial para que o Titular possa provar que os atributos da credencial lhe pertencem.

Após receber o pedido para a emissão de uma credencial, o Emissor verifica se esse pedido está em conformidade com a oferta que enviou anteriormente e, caso não sejam encontrados problemas, emite uma credencial com os atributos acordados e envia-a ao Titular. Por fim, ao receber a credencial, o Titular deverá notificar o Emissor que recebeu a credencial através do sub-protocolo de ACKs (HARDMAN, 2021),

terminando assim o protocolo de emissão da credencial.

### 2.3.3 Protocolo de apresentação verificável (provas)

As apresentações verificáveis desempenham um papel essencial, permitindo que em diversas situações, um Titular acesse serviços fornecidos por uma entidade ao comprovar que possui atributos específicos. Além disso, essas apresentações têm a função crucial de autenticar os dados do Titular, assegurando a veracidade e integridade das informações compartilhadas. Esta prova envolve duas entidades: o Titular e o Verificador. O protocolo de apresentação de prova (KHATEEV, 2019b) busca padronizar as interações entre essas duas entidades, permitindo que o Titular não só demonstre ao Verificador a posse de determinados atributos, mas também confirme a autenticidade das informações fornecidas.

O diagrama de fluxo da Figura 10 representa o processo de geração e validação de uma prova. O protocolo de apresentação da prova pode ser iniciado com a apresentação de uma proposta, por parte do Titular, ou com um pedido de prova, por parte do Verificador. Se o Titular iniciar o protocolo, deverá enviar uma proposta na qual indica os atributos que quer provar. Ao receber a proposta, o Verificador decide se pretende ou não requisitar essa prova ao Titular.

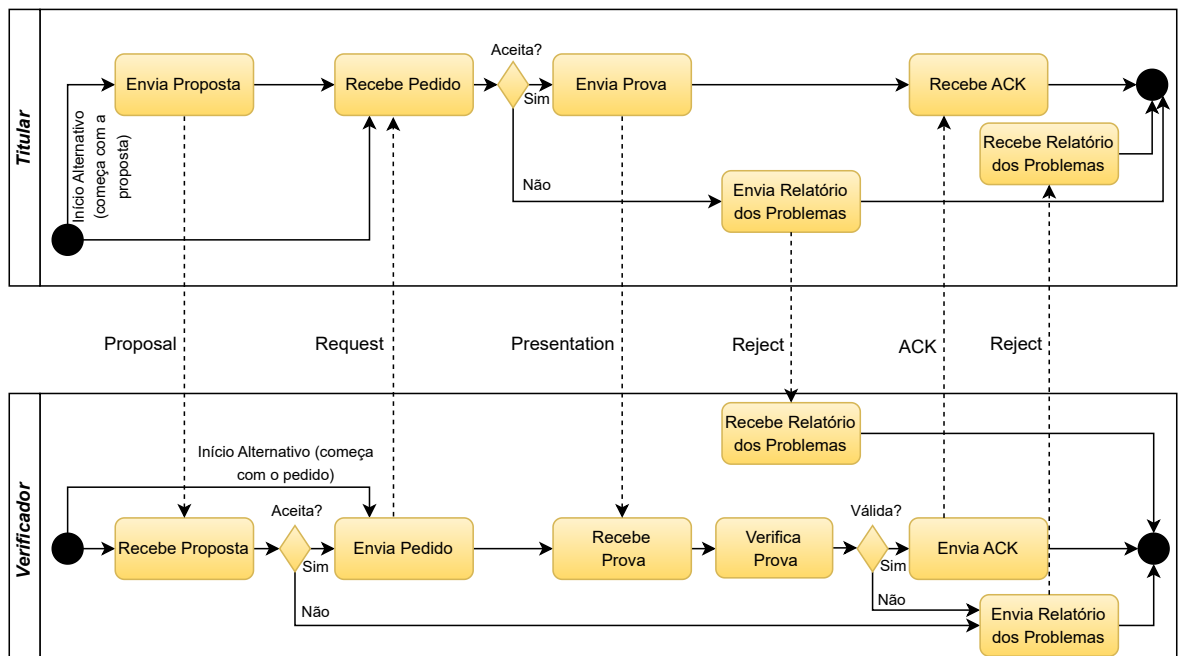


Figura 10 – Protocolo de apresentação da prova

Fonte: (PEIXOTO, 2021)

Em alternativa, o Verificador pode tomar a iniciativa e iniciar o protocolo, enviando um pedido de prova ao Titular. Este pedido de prova deverá conter os nomes dos atributos pretendidos, um conjunto de restrições para cada um destes atributos

(*i.e.* esquemas, emissores e definições de credenciais aceites) e, opcionalmente, um intervalo de tempo para cada atributo, no qual a prova desse atributo deve ser válida, *i.e.*, não esteja revogada. Caso este intervalo não seja especificado, será utilizado o momento em que o pedido de prova for criado.

Em geral a segunda alternativa é a mais utilizada. Após receber o pedido de prova, o Titular verifica os atributos requeridos pelo Verificador e escolhe que credenciais deseja utilizar para cada um desses atributos. Caso não concorde em fornecer certos atributos, ou não possua credenciais válidas com os atributos desejados, deverá rejeitar o pedido e informar o Verificador.

Se o Titular possuir todos os atributos necessários e concordar com a partilha dos mesmos, deverá gerar uma apresentação verificável e enviá-la ao Verificador. Recebendo a apresentação, o Verificador procede a verificação da mesma e, se a prova for válida, informa o Titular de que recebeu e validou a apresentação sem encontrar problemas, através do sub-protocolo ACKs (HARDMAN, 2021), terminando assim o protocolo.

## 2.4 CONSIDERAÇÕES PARCIAIS

O objetivo final de toda arquitetura SSI é alcançar um nível de confiança mutuamente aceitável entre quaisquer partes interagindo na Internet. A base para essa camada de confiança é primeiramente estabelecida pela confiança criptográfica, *i.e.*, pelo enraizamento de DIDs e chaves públicas, resolvíveis publicamente para emissores de credenciais, em uma rede descentralizada.

Mas a confiança criptográfica não é a confiança humana. Essa camada de confiança humana em cima da confiança criptográfica é alcançada no modelo SSI com o uso das credenciais verificáveis. Porém, confiar nas credenciais de um emissor, sem uso de uma padronização, não é escalável. E este foi o mesmo problema enfrentado nos primeiros dias de cartões de crédito na década de 1960, quando cada grande banco tentou emitir sua própria marca de cartão de crédito, e os comerciantes ficaram sobrecarregados, pois não conseguiam lidar com centenas de cartões de crédito diferentes de centenas de bancos diferentes. Assim, a adoção do cartão de crédito não decolou até que os bancos se uniram e formaram redes de cartão de crédito (*e.g.*, Visa e MasterCard), regidas por um conjunto de regras comerciais, legais e técnicas. Esse é o papel das estruturas de governança.

Dessa forma, esses blocos de construção que compõem a arquitetura central de uma solução SSI permitem uma disrupção de outros modelos de gerenciamento de identidades que, até aqui, por definição, dependiam de uma autoridade centralizada para validar e verificar a identidade de pessoas, organizações e coisas, nem sempre

respeitando o controle e privacidade do portador dessa identidade.

Em termos de comparação, em estruturas de identidade isoladas, centralizadas e federadas, as identidades não estão sob o controle da entidade que eles identificam, mas sim, são emitidas por autoridades externas que decidem, a quem ou a que se referem, e quando podem ser revogadas. Além disso, são úteis apenas em determinados contextos e reconhecidas apenas por alguns órgãos, bem como podem desaparecer, ou deixar de ser válidas, se a autoridade externa que as emitiu deixar de existir. Também podem revelar informações pessoais desnecessariamente e podem ser replicadas de forma fraudulenta e declaradas por terceiros mal-intencionados. No aspecto de usabilidade, nomes de usuário e senhas dificultam a existência online das entidades na medida em que muitas vezes essas informações são mantidas em planilhas pessoais, ou em aplicativos de gerenciamento de senhas. Independentemente da solução, as identidades tornam-se um dos pontos mais fracos da atual infraestrutura de segurança cibernética.

Importante observar que o foco principal de todos os exemplos de utilização da arquitetura SSI, especificamente da Camada 3, têm sido a sua utilização para uso humano, ou no âmbito de dispositivos de IoT. Porém, analisando conceitos e especificações, fica clara a **não** existência de limitações, no sentido de estender o seu uso para entidades que podem ser **pessoas, organizações** ou **coisas**. Sendo uma 'coisa' qualquer objeto ou ser inanimado, de natureza real ou abstrata, entende-se que a sua utilização pode ser explorada além do âmbito pessoal ou da IoT, beneficiando outras relações que exigem confiança.

### 3 CADEIA PRODUTIVA DO ALGODÃO

A cultura do algodão tornou-se uma das principais *commodities* brasileiras e, devido ao crescimento e desenvolvimento dos sistemas de produção, apresenta elevado destaque no agronegócio brasileiro, contribuindo para a economia do país e favorecendo a ocupação do Brasil como quinto maior exportador de algodão em escala mundial (COMMITTEE, 2023).

Apesar do volume de exportações expressivo, o Brasil passa por frequentes exigências de documentação que comprovem a certificação de qualidade das *commodities*. Muitos fatores podem estar contribuindo para que isto ocorra, um deles está relacionado com episódios de barreiras sanitárias nas exportações brasileiras de carnes para a Europa e Ásia; outro fator pode estar ligado a busca constante dos consumidores pela qualidade e sustentabilidade. É fato que, à medida que a renda *per capita* aumenta, o grau de exigência por qualidade dos produtos consumidos tende a crescer na mesma velocidade (CONCEIÇÃO; BARROS, 2005).

#### 3.1 ETAPAS DA CADEIA ALGODOEIRA

A cadeia produtiva de algodão se caracteriza como uma das mais longas e complexas, sendo constituída por inúmeras etapas desde a produção primária até o consumidor final (BUAINAIN et al., 2007). A Figura 11 apresenta uma representação esquemática dos grandes blocos da cadeia produtiva algodoeira. Basicamente, o processo de produção pode ser dividido em três grandes blocos, sendo o primeiro composto pela produção (cottonicultura) e beneficiamento (algodoeiras), que sustentam o mercado interno e externo de algodão em pluma; o segundo, abrange as indústrias têxteis e o terceiro é formado pelas confecções (FERREIRA et al., 2022).



Figura 11 – Cadeia Produtiva do Algodão - Visão Macro dos Grandes Blocos.

Fonte: Autor

Os insumos correspondem aos recursos necessários à produção agrícola. Nesse contexto, encontram-se os fornecedores de sementes, fertilizantes, defensivos

e corretivos, implementos agrícolas, colheitadeiras, tratores e caminhões, entre outros (NEVES; PINTO, 2017). A etapa de produção dentro da fazenda engloba a produção de pluma, caroço e fibrilha e inclui o beneficiamento do algodão (FERREIRA et al., 2022). O beneficiamento, que configura-se como a etapa prévia à industrialização, é fundamental na cadeia produtiva do algodão pois envolve a separação das fibras das sementes de forma mecânica, resultando na produção dos fardinhos de algodão em pluma. É crucial ressaltar que a preservação da qualidade da fibra durante o beneficiamento é de extrema importância para obter um algodão que atenda às exigências da indústria têxtil, bem como do mercado externo (AMIPA, 2023).

Nesse processo, também é importante garantir a identificação adequada dos fardinhos produzidos. Para isso, são utilizadas etiquetas que acompanham cada fardo ao longo de sua existência, contendo informações importantes sobre sua origem, qualidade e características específicas. Além disso, um laudo de classificação visual e análise com o auxílio de tecnologia como o *High Volume Instrument* (HVI) são realizados para avaliar a qualidade do algodão contido no fardo. Caso o algodão seja certificado, os selos de certificação também acompanham os fardinhos. Esses selos representam um reconhecimento externo e confiável de que o algodão contido nos fardinhos atende a determinados critérios de qualidade, sustentabilidade, origem ou outros padrões específicos estabelecidos pelas certificadoras.

A confiabilidade das informações nesse processo desempenha um papel crucial. As informações registradas nas etiquetas e presentes nos laudos de classificação, bem como nos selos de certificação, devem ser precisas e confiáveis, pois são utilizadas pelos produtores, compradores e demais agentes da cadeia produtiva para tomadas de decisão e para garantir a transparência e qualidade do produto final. Através dessas informações confiáveis, é possível garantir a rastreabilidade do algodão desde a sua origem, o que é fundamental tanto para atender às exigências dos clientes quanto para cumprir as regulamentações internacionais. Além disso, a precisão dessas informações é fundamental para a correta precificação do algodão, garantindo uma negociação justa e equitativa entre produtores e compradores.

Após a produção dentro das fazendas algodoeiras, os próximos agentes da cadeia algodoeira englobam os fabricantes de especialidades têxteis, a indústria de papel e celulose, a indústria química e de algodão hidrófilo, as indústrias de biodiesel, de ração animal e de alimentos, que processam o caroço do algodão, gerando outros subprodutos.

Na etapa seguinte a produção na fazenda, os fardinhos de algodão em pluma são direcionados para as indústrias têxteis, formadas pelas indústrias de fiação, tecelagem e malharia, ou são comercializados no mercado externo. Caso comercializados no mercado externo, a operação pode ser intermediada por um corretor (*trader*). O

corretor desempenha um papel fundamental na exportação do algodão, atuando como intermediário entre os produtores de algodão brasileiros e os compradores internacionais, facilitando as transações comerciais entre as partes, buscando oportunidades de negócio, negociando contratos e coordenando a logística envolvida na exportação.

Caso seja destinada às indústrias têxteis, o algodão é encaminhado para a primeira etapa do processo industrial, a fiação. Nessa etapa, os fios são produzidos e servem de matéria-prima para as tecelagens ou para as malharias (COSTA; ROCHA, 2009). A tecelagem é responsável pela fabricação de tecidos planos, ao passo que a malharia representa a produção de malhas. Em seguida, os tecidos e malhas fabricados passam pelo beneficiamento têxtil, *i.e.*, recebem tratamentos para a retirada de impurezas e aquisição de características sensoriais e de conforto (SOARES et al., 2010).

Após a etapa de beneficiamento têxtil os tecidos e malhas seguem para as confecções. Nesta etapa, os produtos podem ser divididos em artigos de vestuário ou artigos para o lar (cama, mesa, banho, limpeza e decoração) ou também podem ser destinados ao uso industrial (embalagens, interior de veículos, entre outros). As peças confeccionadas seguem então para o sistema de distribuição até chegar ao consumidor final (COSTA; ROCHA, 2009).

## 3.2 ESTUDOS RELACIONADOS

Nas últimas décadas, os pesquisadores têm se preocupado em desenvolver várias abordagens para alcançar a rastreabilidade e auditabilidade nas cadeias produtivas em geral, cada qual aplicando métodos diferentes. Por meio de uma Pesquisa Bibliográfica Sistemática (PBS) na literatura, buscou-se identificar a existência de trabalhos similares que abordassem as áreas foco deste trabalho: cadeia produtiva ou de *supply chain*, rastreabilidade e confiabilidade, SSI e algodão, com o objetivo de analisar tendências em relação aos problemas existentes. Dessa forma, esse mapeamento tem foco na coleta e categorização de dados, visando melhor entendimento das tendências de publicação nessas áreas.

### 3.2.1 Definição dos Termos de Pesquisa

O fraseamento, com o estabelecimento de palavras-chave, foi estabelecido para a seleção dos trabalhos usando-se os termos: (*"productive chain"OR "supply chain"*) AND (*traceability OR confiability*) AND *"self-sovereign identity"AND cotton*).

No entanto, para essa frase de busca não foram encontrados artigos publicados, de forma que foi necessária uma adaptação para a aplicação nos Mecanismo de Busca Acadêmicas (MBAs), buscando publicações que apresentem soluções para

rastreabilidade e confiabilidade em cadeias produtivas ou de *supply chain* de modo geral. Testes e ajustes foram realizados e a frase de busca para os trabalhos relacionados ficou definida da seguinte forma: (*"productive chain"OR "supply chain" AND traceability OR confiability*).

### 3.2.2 Seleção

O processo de seleção é uma das principais etapas para um levantamento de trabalhos relacionados adequado, levando-se em consideração a recomendação em (GALVÃO; PANSANI; HARRAD, 2015). Há nele quatro fases relevantes:

- Identificação: nesta etapa são elencados o número de trabalhos identificados nos MBAs.
- Seleção: aqui são excluídos os trabalhos idênticos, mesmo que coletados em MBAs diferentes ou até mesmo publicados em veículos diferentes, sendo possível obter-se um número inicial de trabalhos elegíveis à próxima etapa.
- Elegibilidade: nesta etapa tornam-se elegíveis para a pesquisa apenas os trabalhos mais recentes, com data de publicação desde 2020 até o presente, e escritos na língua inglesa, garantindo que as informações estejam atualizadas e reflitam as últimas pesquisas e avanços no tema.
- Inclusão: depois de coletados os trabalhos, levando-se em conta as especificidades mencionadas na elegibilidade, serão elencados critérios de inclusão e exclusão, obtendo-se, por fim, o número de estudos incluídos em síntese quantitativa.

### 3.2.3 Fontes

As fontes de busca do mapeamento serão feitas em MBAs que atendam aos seguintes critérios: mecanismos de busca voltados à tecnologia da informação e engenharias ou mecanismos de busca de caráter multidisciplinar, dentre os quais, os selecionados foram *Science Direct*, *ACM Digital Library* e *IEEE Xplore*, devido à disponibilidade de recursos avançados de busca, acessibilidade aos trabalhos e melhores visualizações dos dados.

### 3.2.4 Análise

Para a triagem dos trabalhos que passaram pela etapa de seleção, são definidos os seguintes critérios de inclusão (CI) e exclusão (CE).

- Critério de Inclusão 01 (CI01): Incluir apenas trabalhos publicados nos últimos três anos (desde 2020 até o presente).
- Critério de Inclusão 02 (CI02): Incluir apenas trabalhos que abordem o tema da rastreabilidade e confiabilidade em cadeias produtivas.
- Critério de Inclusão 03 (CI03): Incluir apenas trabalhos escritos na língua inglesa.
- Critério de Exclusão 01 (CE01): Excluir trabalhos que não estejam relacionados à cadeia do agronegócio ou agroalimentar.

### 3.2.5 Execução

Na busca geral dos mecanismos eleitos como fontes, foram encontrados um total de 632 artigos que atendem à pesquisa usando o fraseamento definido. O resultado da busca apresenta uma tendência de aumento no número de publicações em cada ano, o que assevera que o tema está em ascensão. Essa tendência de crescimento nas publicações permeia todos os mecanismos de buscas utilizados.

### 3.2.6 Elegibilidade

Para determinar a elegibilidade dos trabalhos, foram aplicados os passos de filtragem, tais como retirar os trabalhos repetidos e aplicar os critérios de inclusão e exclusão. Na sequência, são incluídos numa síntese qualitativa, cujo conteúdo do resumo e principais tópicos da publicação são avaliados, resultando nos trabalhos incluídos na síntese quantitativa final. Por fim, chegou-se à apreciação de 5 trabalhos que se tornaram elegíveis à pesquisa e objetos de discussão.

## 3.3 DISCUSSÃO

A cadeia produtiva do algodão consiste em uma grande e complexa rede de entidades (partes interessadas), etapas e processos. A maioria dos trabalhos identificados nos MBAs, adotam uma abordagem centralizada, ou descentralizada com a aplicação da tecnologia blockchain, para alcançar a rastreabilidade das cadeias. A análise dos trabalhos objetos dessa discussão segue conforme:

- Cocco et al. (COCCO; TONELLI; MARCHESI, 2021) apresentam um sistema baseado em SSI para apoiar as cadeias de abastecimento de alimentos, focado na visibilidade das certificações alimentares. O sistema é implementado combinando *Self-Sovereign Identity* (SSI), blockchain Ethereum (ETHEREUM, 2023) e *InterPlanetary File System* (IPFS) e fornece visibilidade para certificações de processos e alimentos, atualmente emitidas por órgãos certificadores aprovados, e entregues e armazenadas em papel por vários participantes na cadeia

de abastecimento de alimentos. No entanto, o sistema em questão não utiliza carteiras digitais e credenciais verificáveis para armazenar as certificações; em vez disso, opta pelo IPFS.

- Agrawal et al. (AGRAWAL et al., 2021) investigam e propõe uma estrutura de rastreabilidade baseada em blockchain, para a cadeia de suprimentos do setor têxtil e de vestuário. Os autores usam contratos inteligentes para capturar as interações entre as partes interessadas da cadeia, e o livro-razão distribuído para armazenar e autenticar as transações, tendo como principal resultado uma simulação que mostra como alcançar rastreabilidade. Segundo os autores, embora a solução fornecida seja projetada para o setor têxtil e de vestuário, ela pode ser adaptada para atender qualquer setor da cadeia de suprimentos, aplicando as modificações necessárias. Vale ressaltar que, apesar deste trabalho propor uma solução de rastreabilidade para a cadeia de suprimentos têxtil e de vestuário, a abordagem sugerida não incorpora SSI.
- Hader et al. (HADER et al., 2022) propõe um *framework* de *Big Data* integrado à uma blockchain, para rastreabilidade da cadeia de suprimentos têxtil, que oferece uma plataforma de informações para todos os agentes da cadeia, com transparência e compartilhamento de informações. Segundo os autores, a integração das duas tecnologias permite gerenciar a rastreabilidade e o compartilhamento de informações com mais precisão. No entanto, o trabalho não aborda aspectos relacionados à privacidade da informação, e a solução não incorpora SSI.
- Sezer et al. (SEZER; TOPAL; NURIYEV, 2022) apresentam uma estrutura para rastreabilidade da cadeia de suprimentos que preserva a privacidade de terceiros usando contratos inteligentes e uma blockchain permissionada. A estrutura promete rastreabilidade e auditabilidade nas transações, no entanto, não se baseia em SSI.
- Por fim, Malik et al. (MALIK et al., 2021) propõe uma estrutura de preservação de privacidade chamada TradeChain, que separa a identidade e os eventos comerciais dos atores da cadeia de suprimentos, gerenciando duas blockchains separadas. Uma blockchain utiliza uma estrutura pública, e é destinada a registrar as identidades dos atores da cadeia de suprimentos, preservando a privacidade e utilizando as características descentralizadas da SSI; enquanto a outra é uma blockchain permissionada, especificamente destinada a registrar eventos da cadeia de suprimentos. Nas transações registradas na blockchain de eventos da cadeia de suprimentos, os atores usam Identificadores Descentralizados (*Decentralized Identifiers* (DIDs)) para provar sua verdadeira identidade. Apesar

de utilizar SSI para verificar as identidades dos atores, o conceito não é aplicado aos eventos da cadeia de suprimentos, como proposto no COTTONTRUST.

Embora a tecnologia blockchain ofereça maiores benefícios para a rastreabilidade de cadeias produtivas, quando comparada às abordagens centralizadas, a mesma também apresenta alguns desafios e problemas que devem ser considerados. Alguns dos problemas associados ao uso da tecnologia blockchain para a rastreabilidade de cadeias produtivas são:

- Escalabilidade: à medida que o número de transações e participantes aumenta, a rede pode ficar congestionada e enfrentar problemas de desempenho. Isso pode afetar a capacidade de processamento e a velocidade das transações, dificultando a adoção em larga escala.
- Custos: a manutenção da rede, a validação das transações e a armazenagem dos dados requerem recursos significativos, como poder computacional e energia elétrica. Isso pode ser um obstáculo para empresas de menor porte ou com recursos limitados.
- Privacidade e proteção de dados: a natureza transparente e imutável da tecnologia blockchain pode criar desafios em relação à privacidade e proteção de dados sensíveis. Embora seja possível utilizar técnicas de criptografia para proteger os dados, ainda existem preocupações em relação ao acesso indevido e à exposição de informações confidenciais.
- Conformidade com as leis gerais de proteção de dados: a tecnologia blockchain é conhecida por sua natureza imutável e distribuída, o que pode dificultar a conformidade com as regulamentações de privacidade de dados como a LGPD e GDPR.

Esses problemas destacam a importância de explorar outras alternativas descentralizadas, como a utilização do SSI, para superar as limitações das abordagens centralizadas ou das que utilizam a tecnologia blockchain, e promover uma rastreabilidade mais confiável, transparente e resistente a falhas na cadeia produtiva do algodão.

A Tabela 3 apresenta uma comparação entre os trabalhos relacionados e o COTTONTRUST, abordando aspectos cruciais relacionados à autonomia e controle das entidades na gestão de seus dados pessoais, à capacidade de proporcionar rastreabilidade em tempo real dos dados, à habilidade de verificar a autenticidade dos dados em tempo real e ao cumprimento das regulamentações de proteção de dados. Ao examinar essa comparação, destaca-se que o COTTONTRUST se apresenta como

Tabela 3 – Critérios de Avaliação - Comparação entre os trabalhos relacionados.

	Cocco et al. (COCCO; TONELLI; MARCHESI, 2021)	Agrawal et al. (AGRAWAL et al., 2021)	Hader et al. (HADER et al., 2022)	Sezer et al. (SEZER; TOPAL; NURIYEV, 2022)	Malik et al. (MALIK et al., 2021)	COTTON TRUST
<b>Autonomia e controle das entidades no gerenciamento de seus dados pessoais.</b>	Não	Não	Não	Não	Não	Sim
<b>Capacidade de fornecer rastreabilidade em tempo real dos dados.</b>	Não	Sim	Sim	Sim	Não	Sim
<b>Capacidade de verificar a autenticidade dos dados em tempo real.</b>	Sim	Não	Não	Não	Sim	Sim
<b>Conformidade com as leis gerais de proteção de dados.</b>	Não	Não	Não	Não	Sim	Sim

uma solução abrangente, lidando de maneira eficaz com todos os aspectos mencionados.

### 3.4 CONSIDERAÇÕES PARCIAIS

A PBS foi realizada para o melhor entendimento das tendências de publicação nas áreas focos deste trabalho: cadeia produtiva ou de *supply chain*, rastreabilidade e confiabilidade, SSI e algodão. A pesquisa consultou 3 MBAs com 632 retornos, nos quais, após refinamento, resultaram em 5 estudos que foram explorados completamente.

Analisando os trabalhos objetos da discussão, é possível observar que, embora abordem a questão da rastreabilidade nas cadeias produtivas, os trabalhos falham em abordar aspectos relacionados com as leis gerais de proteção de dados. Além disso, a verificabilidade dos selos de certificação é esquecida, bem como abordagens para a auditabilidade específica dos produtos. Esses aspectos devem ser levados em consideração para projetar um sistema que se aplique às cadeias produtivas.

Dessa forma, não houveram trabalhos preenchendo todos os requisitos derivados do problema de pesquisa foco deste trabalho, mostrando-se indícios de uma lacuna de pesquisa, e lastreando a proposta nos requisitos levantados no problema e não resolvidos nos trabalhos relacionados. As considerações inerentes à proposta de resolução do problema podem ser encontradas no Capítulo 4.

## 4 COTTONTRUST

Com o objetivo de propor uma solução aos problemas existentes e abordar de forma abrangente os desafios de se alcançar rastreabilidade, confiabilidade e verificabilidade na cadeia produtiva do algodão, uma estrutura baseada no modelo SSI denominada COTTONTRUST, é apresentada neste trabalho. O COTTONTRUST é uma arquitetura descentralizada fundamentada no modelo *Self-Sovereign Identity* (SSI), implementada por meio da blockchain Hyperledger Indy, com o objetivo de alcançar rastreabilidade, confiabilidade e verificabilidade na cadeia produtiva do algodão. Para o *design* do sistema, foi adotada uma abordagem que conceitua a cadeia de produção de algodão como uma rede interconectada de nós (entidades participantes na cadeia). Para exemplificar, a Figura 12 abrange a produção e comercialização de fardos de algodão.

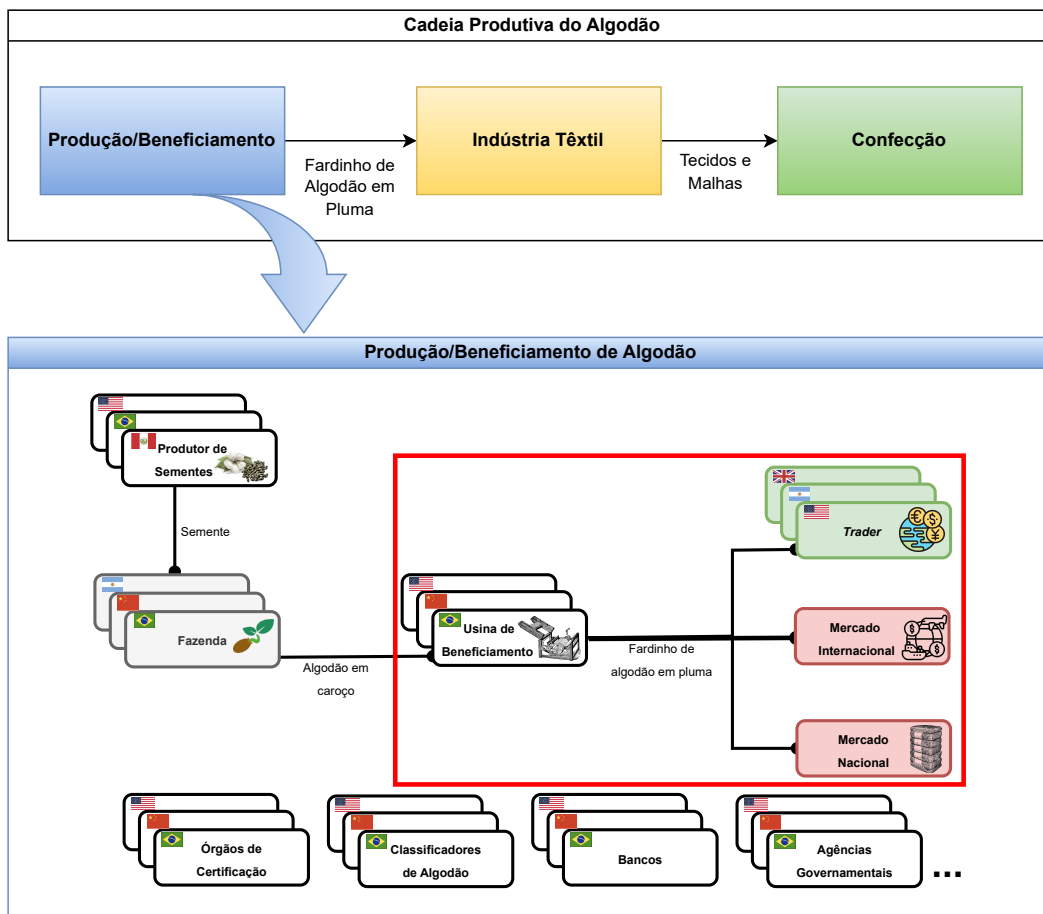


Figura 12 – Cadeia Produtiva do Algodão (em destaque as fases de beneficiamento e comercialização de fardos de algodão em pluma).

Fonte: Autor

Embora os processos subjacentes em cada fase possam variar, a operaciona-

lidade do sistema permanece consistente ao longo de toda a extensão da cadeia de produção. As entidades participantes na cadeia, foco deste trabalho, incluem:

- Produtor de Sementes: responsável pela produção de sementes de algodão.
- Fazenda: local onde ocorre o cultivo de algodão.
- Unidade de Beneficiamento de Algodão (UBA): responsável pelo processamento do algodão colhido, separando as fibras das sementes e montando fardos de algodão para comercialização.
- *Trader*: envolvido na negociação e comércio de algodão, atuando como intermediário entre produtores, UBAs e compradores.
- Mercado Internacional: representando entidades ou empresas localizadas fora do país que adquirem algodão para diversos fins, como produção têxtil.
- Mercado Nacional: representando entidades ou empresas dentro do país que adquirem algodão para diversos fins, incluindo produção têxtil ou outros usos industriais.
- Órgãos Certificadores: responsáveis por certificar que o algodão atende a padrões específicos de qualidade, sustentabilidade ou origem.
- Classificadores de Algodão: especialistas credenciados que avaliam e classificam o algodão com base em características como qualidade, tipo de fibra e outras especificações relevantes.

Por natureza, a cadeia de produção de algodão é inerentemente descentralizada, conforme evidenciado na Figura 12, alinhando-se aos princípios do SSI. Cada entidade na cadeia pode estar localizada em regiões geograficamente distantes, mesmo em países diferentes, enfatizando a importância da descentralização e destacando os benefícios potenciais do uso do SSI para promover transparência e confiabilidade em um cenário caracterizado por uma ampla dispersão geográfica. Embora cada entidade na cadeia tenha características específicas, do ponto de vista técnico, elas podem ser abstraídas de maneira semelhante. Neste trabalho, essas unidades operacionais são designadas como COTTON-CELL.

De modo a explicar a solução desenvolvida, a Seção 4.1 apresenta a arquitetura e oferece uma visão geral dos componentes que constituem o sistema e como estes se relacionam entre si. Na sequência, a Seção 4.2 apresenta a dinâmica funcional do COTTONTRUST e por fim, a Seção 4.3 apresenta o funcionamento das principais transações que ocorrem no contexto do COTTONTRUST, destacando as interações e processos fundamentais que impulsionam a cadeia produtiva do algodão.

#### 4.1 COTTON-CELL - COMPONENTES E ESTRUTURA

Cada entidade da cadeia possui uma estrutura chamada COTTON-CELL, cuja perspectiva é exemplificada na Figura 13. O foco dessa estrutura está na Camada 3 da Pilha SSI, detalhada no Capítulo 2, Seção 2.2, e envolve os seguintes componentes principais:

- Identificadores Descentralizados (DIDs).
- Agentes e Carteiras Digitais.
- Registro de Dados Verificável (RDV).
- Credenciais e Apresentações Verificáveis.

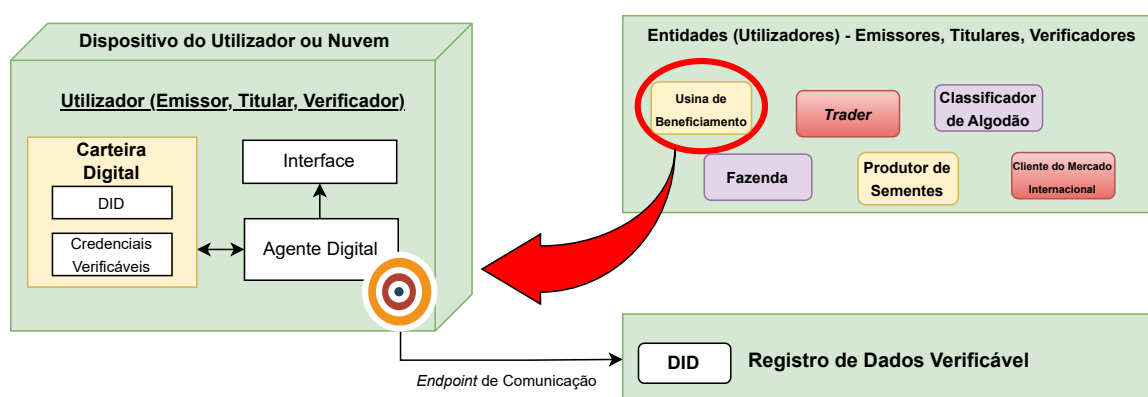


Figura 13 – Arquitetura do COTTONTRUST

Fonte: Autor

Além disso, essa arquitetura incorpora três classes de entidades claramente diferenciadas: Emissores, Titulares e Verificadores, os quais também são referidos como **Utilizadores** em certas Seções do trabalho. Conforme a situação e a transação em curso, essas entidades assumem os papéis de Emissores, Titulares e Verificadores, adaptando-se ao contexto específico da interação. Na sequência, cada componente é detalhadamente abordado.

#### Identificadores Descentralizados (DIDs)

Cada entidade é identificada por um *Decentralized Identifier* (DID) público, que é imutavelmente registrado no RDV. DIDs públicos desempenham a função de identificadores exclusivos, garantindo uma representação digital única para cada entidade na

cadeia de algodão, e seguem a sintaxe padrão definida pelo W3C em *Decentralized Identifier* (DID) v1.0 (SPORNY et al., 2021). A Figura 14 apresenta um exemplo de um DID público para a entidade UBA.

**did:mybc:TsiaIUYBJPxVBnz8w2B5gb**

DID público

Figura 14 – Exemplo de DID Público da entidade UBA

Como é possível observar na figura, o DID indica o esquema no qual está inserido (*did*), qual é o seu método (localização do documento DID - *mybc*) e qual é a especificação desse método (endereço no qual o documento DID se encontra). O método *mybc* corresponde ao RDV utilizado nesta solução, de forma que o sistema irá buscar o documento com o identificador *TsiaIUYBJPxVBnz8w2B5gb* neste local.

Cada DID possui um documento associado que contém dados referentes ao identificador, tais como: chaves públicas de autorização e autenticação, serviços disponibilizados e os respectivos *endpoints* de comunicação, entre outros. A Figura 15 exemplifica o documento associado ao DID público apresentado na Figura 14.

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:mybc:TsiaIUYBJPxVBnz8w2B5gb",
  "publicKey": [
    {
      "controller": "did:mybc:TsiaIUYBJPxVBnz8w2B5gb",
      "id": "did:mybc:TsiaIUYBJPxVBnz8w2B5gb#1",
      "publicKeyBase58": "FfMSUfKQqUh7dEJngltEuppXMvrD1Ef6RScR3jgZykwY",
      "type": "Ed25519VerificationKey2018"
    }
  ],
  "authentication": [
    "did:mybc:TsiaIUYBJPxVBnz8w2B5gb#1"
  ],
  "service": [
    {
      "id": "did:mybc:TsiaIUYBJPxVBnz8w2B5gb#agent",
      "recipientKeys": [
        "FfMSUfKQqUh7dEJngltEuppXMvrD1Ef6RScR3jgZykwY"
      ],
      "routingKeys": [],
      "serviceEndpoint": "http://localhost:5001",
      "type": "agent"
    }
  ]
}
```

Figura 15 – Documento do DID *did:mybc:TsiaIUYBJPxVBnz8w2B5gb*

Nesta figura é possível observar que o documento segue o esquema definido em <https://w3id.org/did/v1>, tal como está indicado na propriedade *@context*. A propriedade *id* indica o DID ao qual o documento pertence. Em seguida são apresentadas a propriedade *publicKey*, que consiste em uma lista de chaves públicas de autorização,

e a propriedade *authentication*, que consiste em uma lista de chave públicas de autenticação. Por fim, a propriedade *service* descreve todos os serviços disponibilizados pelo DID.

### **Agentes e Carteiras Digitais**

Todas as entidades são responsáveis por manter credenciais verificáveis, DIDs e chaves privadas em sua posse. Para esse fim, cada entidade possui uma carteira digital que desempenha o papel de armazenar essas informações e permitir seu uso conforme necessário. Usualmente a carteira digital é instalada no dispositivo que a entidade utiliza para interagir com o sistema, no entanto, há também a possibilidade de utilizar carteiras digitais armazenadas em serviços de nuvem.

Os agentes digitais atuam como intermediários, permitindo que as entidades interajam com o ecossistema. Para isso, incluem um componente de processamento central, que contém toda a lógica operacional, e uma interface destinada à interação com o Utilizador, para auxiliá-lo na interação com as demais entidades, facilitando o processo de emissão/aquisição de credenciais verificáveis e a exibição/verificação de apresentações verificáveis. A comunicação do agente digital com outros agentes e com o RDV é estabelecida através de *endpoints* de comunicação. Cabe ao agente digital executar diversas funções em nome do seu Utilizador, dentre elas:

- Solicitar a emissão de uma credencial verificável, aceitar a credencial emitida e armazená-la na carteira.
- Receber uma solicitação para comprovação de informações de uma credencial e entregá-la ao Verificador.
- Aceitar as mensagens de notificação recebidas por uma conexão e processar qualquer ação resultante.
- Enviar mensagens assinadas digitalmente para suas conexões.

Os agentes digitais são divididos em duas categorias de acordo com a sua localização: agente de nuvem (*cloud agent*) e agente de borda (*edge agent*). Um agente de nuvem, como o próprio nome indica, está hospedado na nuvem, o que lhe permite estar constantemente disponível para receber e enviar mensagens, bem como estabelecer conexões com outros agentes e entidades, enquanto um agente de borda é executado em um dispositivo físico sob o controle do seu proprietário. No COTTONTRUST, o agente e carteira digital utilizado é do tipo agente de borda para todas as entidades, com exceção da entidade **Fardinho** de algodão, que utiliza um

agente e carteira em nuvem, dada a impossibilidade deste de portar um dispositivo físico.

### **Registro de Dados Verificável (RDV)**

O RDV, por sua vez, funciona como uma rede subjacente que atua como um registro imutável de dados, usado para registrar os DIDs e armazenar esquemas de credenciais verificáveis e chaves públicas, oferecendo suporte ao retorno de dados necessários para validar as apresentações verificáveis. No COTTONTRUST, o RDV é composto pela blockchain Hyperledger Indy (INDY, 2022), criada especificamente para o caso de uso das identidades digitais, com o auxílio de dois componentes distintos: Indy Plenum (PLENUM, 2023) e Indy Node (NODE, 2023). O Indy Plenum é responsável pela implementação do protocolo de consenso, enquanto o Indy Node permite efetuar a gestão do *ledger* e dar suporte às transações específicas do sistema. O Anexo C apresenta o Indy de forma mais detalhada.

Inicialmente, os administradores representados pelas entidades do tipo *Trustee*, estabelecem e registram um modelo de governança para a blockchain, definindo uma estrutura de confiança necessária. Essas entidades *Trustee* assumem a responsabilidade de cadastrar na rede os emissores de credenciais, como os órgãos de certificação e os classificadores de algodão, reconhecendo-os como fontes legítimas para a emissão de laudos e selos; bancos; agências governamentais, entre outros. Apenas as entidades mais confiáveis do sistema, *i.e.*, *trustees*, *stewards* e *endorsers* podem ser emissores de credenciais.

### **Credenciais e Apresentações Verificáveis**

Dentro do contexto de COTTON-CELL, as entidades acumulam inúmeras Credenciais Verificáveis associadas ao seu DID público. Essas credenciais abrangem uma variedade de dados relevantes, incluindo selos de certificação, relatórios, conformidade com padrões específicos, laudos, comprovantes, bem como outros documentos essenciais que circulam entre as entidades da cadeia.

A relevância das credenciais verificáveis para o mundo real reside em sua capacidade de fornecer uma representação digital confiável e verificável de informações tangíveis. Exemplificadamente, uma credencial de "Selo de Certificação de Algodão Sustentável", emitida por uma autoridade competente está associada a um DID específico na blockchain. Essa credencial não apenas atesta a qualidade do produto, mas também pode ser verificada por outras partes ao longo da cadeia.

Ao empregar Credenciais Verificáveis, o COTTON-CELL estabelece uma camada de confiança e transparência na cadeia de produção de algodão, oferecendo

a capacidade de verificar a autenticidade e validade das informações em tempo real, sem a necessidade de contato com a entidade emissora. A emissão e verificação de credenciais acontecem de forma a preservar a privacidade com a divulgação seletiva dos valores de seus atributos. Isso não apenas fortalece a integridade da cadeia, mas também facilita a tomada de decisões informadas por parte de produtores, compradores, reguladores e outros participantes envolvidos.

Todas as credenciais seguem esquemas de dados que indicam quais os atributos estas devem conter. No COTTONTRUST os esquemas são armazenados na blockchain e apenas podem ser adicionados no *ledger* pelas entidades mais confiáveis do sistema, *i.e.*, *trustees*, *stewards* e *endorsers*. O Anexo C explica detalhadamente os papéis que as entidades podem possuir, bem como o sistema de permissões. A Figura 16 ilustra um esquema de dados que representa, exemplificadamente, um registro chamado Cadastro Nacional de Pessoa Jurídica (CNPJ) que identifica as pessoas jurídicas no Brasil, com os atributos: número de inscrição, nome empresarial, endereço, data de abertura, natureza jurídica, atividade econômica principal, situação cadastral, entre outros.

```
{
  "id": "schema:mybc:did:mybc:Th7MpTaRZVRYnPiabds81Y:2:identification_card:1.0",
  "name": "identification_card",
  "ver": "1.0",
  "version": "1.0",
  "attrNames": ["inscricao", "nomeEmp", "endereco", "dataAbertura", "natureza", "ativEcon", "situacao"]
}
```

Figura 16 – Esquema de uma credencial referente ao CNPJ

Qualquer Emissor que pretenda emitir credenciais baseadas num dado esquema, deverá primeiramente criar a respectiva definição da credencial, que indica o DID do Emissor e qual esquema será utilizado para emitir as credenciais, bem como quais chaves criptográficas serão usadas para assiná-las. É também na definição da credencial que os Emissores indicam se as credenciais irão ou não suportar revogação. A revogação de credenciais não entrará no escopo deste trabalho, ficando reservado o seu desenvolvimento em trabalhos futuros. A Figura 17 mostra um exemplo da definição de uma credencial baseada no esquema apresentado na Figura 16.

A definição da credencial apresentada é do tipo *CL*, pois recorre ao esquema de assinaturas *Camenisch-Lysyanskaya* (ABRAMSON, 2019) para gerar provas sobre os atributos das credenciais. Esta técnica criptográfica permite utilizar ZKP (detalhado na Seção 2.1.1). Os valores presentes no atributo *primary* correspondem à chave pública associada à chave privada, que o Emissor utiliza para assinar as credenciais referentes à esta definição da credencial. A chave privada correspondente está armazenada na carteira digital do Emissor. Utilizando ambas as chaves, os Verificadores

```

{
  "id": "creddef:...:c727cf04-fffc-4513-alc4-14255f4edce4",
  "schemaId": "l18",
  "type": "CL",
  "tag": "c727cf04-fffc-4513-alc4-14255f4edce4",
  "value": {
    "primary": {
      "n": "100228580668651158692914780765...",
      "s": "196247300449649923814252465523...",
      "r": {
        "master_secret": "350938093289543103383642483660...",
        "inscricao": "823936067762417570855060964959...",
        "nomeEmp": "716761440523030981625464059121...",
        "endereco": "726787698876743479834739121..."
      },
      ...
    },
    "rctxt": "734602727362875873203644824736...",
    "z": "497435813598260173410903751485..."
  },
}

```

Figura 17 – Definição da credencial baseada no esquema da Figura 16

são capazes de validar as provas fornecida pelo Titular, por meio das apresentações verificáveis, advindas dessa credencial.

Após a criação da definição da credencial, o Emissor pode emitir credenciais verificáveis. A Figura 18 mostra a estrutura da credencial verificável relativa ao CNPJ da UBA, emitida por meio da definição da credencial ilustrada na Figura 17. Nesta figura é possível observar um conjunto de metadados tais como os identificadores do esquema e a definição da credencial utilizados. É também possível observar a presença da assinatura do Emissor no atributo *p\_credencial*.

```

{
  schema_id: "schema:mybc:did:mybc:Th7MpTaRZVRYnPiabds81Y:2:identification_card:1.0",
  cred_def_id: "creddef:...:c727cf04-fffc-4513-alc4-14255f4edce4",
  values: {
    inscricao: { raw: "01345678000172", encoded: "9877887732323231443" },
    nomeEmp: { raw: "UBA Fic Ticia", encoded: "4307168083...4218340983" }
  },
  signature: {
    p_credencial: {
      m_2: "353151046837968621381167058800...",
      a: "825684911437287066190078790279...",
      e: "259344723055062059907025491480...",
      v: "604348989985369035181261319997..."
    },
    r_credencial: {
      sigma: "1 239EA...2CE3A 1 1E78E...2F12B 2 095E4...7A8A8",
      c: "019EA760AE2CDB59E6BF6CDD1289E3...",
      vr_prime_prime: "19FB849DBD650CB6DBD022E23A5378...",
      witness_signature: [Object],
      g_i: "1 09611...5AEE7 1 03C0C...3E191 2 095E4...7A8A8",
      i: 1,
      m2: "07CEC39B815BF65EAED7D17B82C5158..."
    }
  },
  signature_correctness_proof: {
    se: "201852721081482002435736939227...",
    c: "617669126379245590734067334966..."
  }
}

```

Figura 18 – Estrutura da credencial baseada na definição da Figura 17

Para um Titular provar que possui certos atributos, o mesmo utiliza-se das

apresentações verificáveis, que permitem ao Titular recorrer a utilização do mecanismo de divulgação seletiva, *i.e.*, podendo agrupar subconjuntos de atributos de várias credenciais numa única apresentação da maneira que achar mais apropriado, gerando as provas para cada um desses atributos. A Figura 19 mostra a estrutura de uma apresentação verificável com as respectivas provas.

```

{
  "proof": {
    "proofs": [
      {
        "primary_proof": { ... },
        "non_revoc_proof": { ... }
      },
      ...
    ],
    "requested_proof": {
      "revealed_attrs": {
        "attributel": {
          "sub_proof_index": 0,
          "raw": "UBA Fic Ticia",
          "encoded": "430716808397556384771159808067..."
        }
      },
      "self_attested_attrs": {},
      "unrevealed_attrs": {},
      "predicates": {
        "predicate1": {
          "sub_proof_index": 0
        }
      }
    },
    "identifiers": [
      {
        "schema_id": "schema:mybc:did:mybc:Th7MpTaRZVRYnPiabds81Y:2:identification_card:1.0",
        "cred_def_id": "creddef:...:c727cf04-fffc-4513-alc-f4edce4",
        "timestamp": 1607468936
      }
    ]
  }
}

```

Figura 19 – Estrutura de uma apresentação verificável

A Figura 20, por sua vez, mostra a estrutura de uma prova primária com os atributos inscrição e nome empresarial. Ao receber a apresentação verificável, o Verificador irá validar a prova de posse dos atributos apresentada através da chave pública presente na definição da credencial criada pelo Emissor, cujo identificador está incluído na apresentação verificável. Para isso, o Verificador deverá obter na blockchain todos os esquemas e definições de credenciais associados aos atributos presentes na apresentação verificável.

## 4.2 FUNCIONAMENTO

Reiterando, ao longo de sua existência, cada entidade acumula inúmeras credenciais, que permanecem armazenadas em sua respectiva carteira digital. Essas credenciais desempenham um papel crucial, servindo como evidência e permitindo que a entidade valide informações específicas quando necessário, fornecendo suporte

```

"primary_proof": {
  "eq_proof": {
    "revealed_attrs": {
      "inscricao": "430716808397556384771159808067..."
    },
    "a_prime": "368284308455951510765534628793...",
    "e": "193318900696657403670256666627...",
    "v": "129239511969463291327727801806...",
    "m": {
      "nomeEmp": "142652048528955707775310921850...",
      "master_secret": "796726123207413788292039893425..."
    },
    "m2": "137488570520550628603772283640..."
  },
  "ge_proofs": [
    {
      "u": {
        "0": "269727644285287929343987538516...", "1": "157071409471924436735198137183...",
        "2": "119137670921893890011657455936...", "3": "622587008850034128884692320255..."
      },
      "r": {
        "0": "118602951220624397246401554811...", "1": "629614649614589803891832893105...",
        "2": "145278787635056442687637415925...", "3": "106703453152164666739626923002...",
        "DELTA": "585086736548664812096052347871..."
      },
      "mj": "142652048528955707775310921850...",
      "alpha": "770041470765173884739766649456...",
      "t": {
        "0": "832400275584670645478597470190...", "1": "465790111471933280508192088553...",
        "2": "143998786310213448397980671440...", "3": "488829997786177528387221611740...",
        "DELTA": "31096582569282775961077002..."
      },
      "predicate": {
        "attr_name": "nomeEmp",
        "p_type": "GE",
        "value": 18
      }
    }
  ]
}

```

Figura 20 – Prova de posse dos atributos

concreto em situações em que é necessário provar determinados fatos ou aspectos de sua identidade. No contexto operacional do COTTONTRUST, a dinâmica funcional é representada na Figura 21(a) e descrita da seguinte forma:

1. As entidades envolvidas na transação estabelecem uma conexão, utilizando o Protocolo de conexão especificado na Subseção 2.3.1 .
2. Uma entidade na cadeia solicita (ou recebe uma oferta de) uma credencial verificável de uma entidade emissora. A entidade emissora, ao receber e aceitar a solicitação, emite a credencial, assinando-a digitalmente com seu DID e chave privada, e a encaminha para a entidade solicitante, que a armazena em sua carteira digital, utilizando o Protocolo de emissão de credencial especificado na Subseção 2.3.2.
3. Em qualquer momento, qualquer entidade na cadeia tem a capacidade de solicitar informações e, se autorizada pelo detentor da credencial, acessar as credenciais de cada participante. Nesse processo, o solicitante direciona a solicitação para a carteira digital do detentor da credencial. A carteira digital, por sua

vez, gera uma prova, que incorpora informações essenciais, incluindo o DID do emissor. Esse DID possibilita a verificação de autenticidade por meio de uma consulta à blockchain para confirmar sua legitimidade. Esse processo é realizado utilizando o Protocolo de apresentação verificável (provas) especificado na Subseção 2.3.3

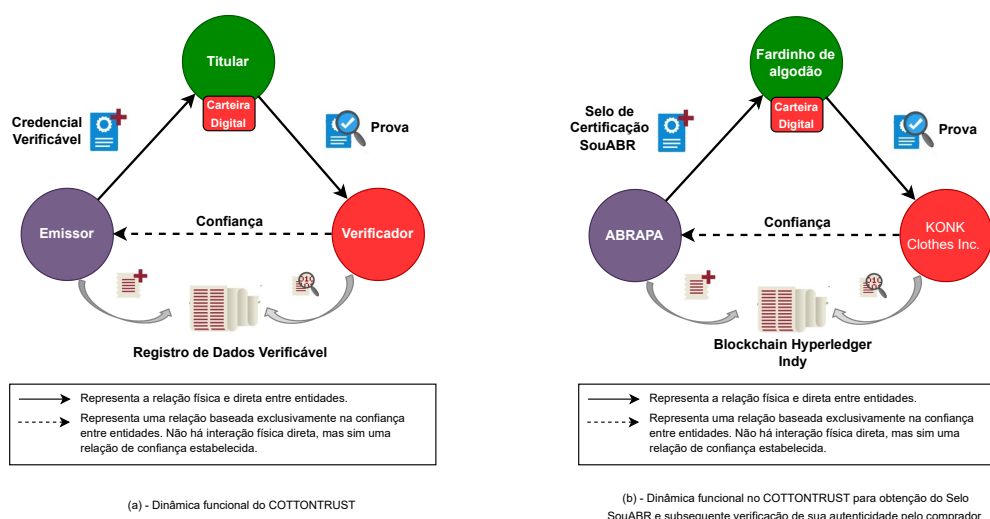


Figura 21 – Dinâmica Funcional no COTTONTRUST - Triângulo da Confiança.

Para facilitar o entendimento, um exemplo relacionado ao Selo de Certificação Sustentável 'SouABR' é demonstrado na sequência. Este selo, no Brasil, é conferido pelo órgão certificador ABRAPA. O procedimento para obter o selo 'SouABR' começa com um processo externo à cadeia, no qual a fazenda produtora solicita uma auditoria de seus processos à ABRAPA, de acordo com os requisitos estabelecidos por essa certificação específica. O algodão produzido pela fazenda certificada, portanto, carregará o selo de certificação 'SouABR', e ao ser vendido à um comprador, este pode verificar se o selo é autêntico e emitido por uma entidade confiável. Para fins de simplificação, presume-se que os seguintes requisitos foram atendidos: (i) As entidades relevantes para o cenário em questão estão devidamente registradas na blockchain, possuindo seus DIDs. (ii) O processo externo à cadeia que envolve a análise para concessão do selo, já foi conduzido e aprovado.

A dinâmica funcional no COTTONTRUST, para a obtenção do selo 'SouABR' e verificação subsequente de sua autenticidade pelo comprador, é representada na Figura 21(b) e descrita da seguinte forma:

1. A ABRAPA emite uma credencial verificável relacionada ao selo de certificação 'SouABR' para o algodão produzido pela fazenda auditada.

2. A credencial do selo 'SouABR' é armazenada na carteira digital do fardo de algodão.
3. O comprador, a empresa KONK Clothes Inc., deseja verificar se o algodão que pretende comprar possui o selo 'SouABR' e se este é autêntico. Portanto, solicita uma prova à carteira digital do fardinho de algodão. Se o fardinho consentir, sua carteira digital gera e retorna as provas ao verificador. A prova contém o DID do emissor (ABRAPA), que o comprador usa para confirmar sua legitimidade na blockchain. Essa operação é realizada em tempo real e não requer contato com a entidade emissora ABRAPA.

### 4.3 COTTON-TRANSACTIONS

O exemplo apresentado, destacando o Selo de Certificação Sustentável 'SouABR', ilustra um cenário simplificado enfocando a verificabilidade e autenticidade de informações na cadeia de produção de algodão. Na prática, várias entidades podem se envolver em cada estágio da cadeia algodoeira. Cada entidade inicia seu envolvimento registrando-se na blockchain, criando seu DID e obtendo sua carteira digital. Isso marca a fase inicial das transações **REG\_ENTITY**, envolvendo operações de escrita no livro-razão. Uma vez registradas, as entidades recebem credenciais verificáveis armazenadas em suas carteiras digitais. Essas credenciais servem como evidência que pode ser usada para validar vários fatos ao longo da cadeia de produção.

Na sequência, durante a venda de fardos de algodão, o comprador adquire produtos da UBA, desencadeando uma nova transação chamada **SELL\_COTTON**. Esta transação incorpora uma consulta à blockchain para verificação de prova. O comprador pode confirmar a autenticidade dos selos de certificação nos fardos de algodão, verificar a origem da fazenda produtora e garantir que as sementes provenham de produtores confiáveis.

Além disso, as seguintes transações desempenham papéis cruciais no sistema:

- **QUERY\_COTTON:** Esta transação permite que os participantes da cadeia produtiva do algodão consultem detalhadamente a rastreabilidade de um determinado fardo de algodão, por meio da consulta às credenciais verificáveis associadas ao fardinho. Ao realizar essa consulta, as entidades podem obter informações específicas sobre a origem do algodão, os processos pelos quais passou, certificações associadas e eventos relevantes ao longo de sua jornada na cadeia produtiva.

- **PROOF\_VERIFY:** Esta transação é essencial para verificar provas na blockchain. Os participantes podem validar a autenticidade de informações específicas, utilizando as evidências e credenciais armazenadas na blockchain. Essa funcionalidade assegura que as transações são autênticas e não foram alteradas, proporcionando confiabilidade às informações presentes na cadeia de produção.
- **REG\_SCHEMA:** Registra o esquema de credenciais verificáveis na blockchain, definindo a estrutura das credenciais que serão utilizadas na cadeia de produção. Isso inclui a especificação dos atributos e suas propriedades.
- **REG\_DEF:** Registra as definições de esquemas de credenciais verificáveis na blockchain, fornecendo as regras e políticas para a emissão e validação das credenciais. Define como os esquemas registrados na transação REG\_SCHEMA devem ser utilizados.
- **QUERY\_SEAL:** Permite a consulta detalhada do selo de certificação de um fardinho de algodão, por meio da consulta às credenciais verificáveis associadas, possibilitando a verificação de autenticidade e integridade do selo.
- **QUERY\_LAUDO:** Permite a consulta detalhada do laudo de classificação do algodão, por meio da consulta às credenciais verificáveis associadas ao fardinho, proporcionando informações sobre a qualidade e características do produto.
- **CONNECT\_ENT:** Esta transação viabiliza a conexão entre duas entidades na cadeia produtiva, permitindo que troquem informações, realizem negociações ou colaborações. Através da CONNECT\_ENT, as entidades podem estabelecer uma relação que facilita a interação e compartilhamento de dados de forma segura.
- **REG\_CREDENTIAL:** Registra a emissão de credenciais para uma entidade específica, indicando os atributos e informações incluídos na credencial.

#### 4.4 CONSIDERAÇÕES PARCIAIS

Este capítulo detalhou a proposta do COTTONTRUST, apresentando os principais conceitos, transações e requisitos fundamentais que guiam o desenvolvimento do sistema. A introdução do Selo de Certificação Sustentável 'SouABR' proporcionou um exemplo prático, ilustrando como o COTTONTRUST pode viabilizar a transparência e confiabilidade desejadas na cadeia produtiva. Cada transação foi detalhadamente explicada, desde o registro inicial das entidades até a venda de fardos de algodão e as consultas associadas.

O próximo capítulo abordará detalhes da análise experimental e discussões de resultados, avançando na compreensão da eficácia do COTTONTRUST na prática. A análise aprofundada desses aspectos contribuirá para a validação da proposta, demonstrando como o sistema pode prover transparência, segurança e confiança na cadeia produtiva do algodão.

## 5 EXPERIMENTAÇÃO E ANÁLISE DE RESULTADOS

Nesta seção, a análise experimental é detalhada, abrangendo o ambiente de teste, descrição do protótipo, plano de teste, resultados e discussões, explorando elementos para avaliar o desempenho e a eficácia do COTTONTRUST. Inicialmente, na Seção 5.1 é apresentado o ambiente de teste no qual os experimentos foram conduzidos, destacando as especificações técnicas e infraestrutura utilizadas para garantir uma análise completa. O protótipo é detalhado na Seção 5.2, especificando os principais fluxos de trabalho da cadeia algodoeira. O plano de teste é detalhado na Seção 5.3, abrangendo os fluxos escolhidos para as medições, tipos de transações investigadas e métricas selecionadas para avaliação de desempenho. Finalmente, na Seção 5.4, é apresentada a discussão e análise dos resultados obtidos, interpretando as métricas coletadas para fornecer *insights* sobre a escalabilidade, eficiência e capacidade do sistema COTTONTRUST em diferentes contextos operacionais.

### 5.1 AMBIENTE DE TESTES

O protótipo do COTTONTRUST foi implantado em uma infraestrutura robusta, garantindo um ambiente propício para a execução eficiente de testes e experimentos. A seguir são detalhadas as especificações e ferramentas utilizadas, proporcionando uma visão abrangente do ambiente de teste:

#### **Especificações da Máquina Física:**

- Memória RAM: 148 GB
- Processador: Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.10GHz
- Núcleos Físicos: 4
- Núcleos Lógicos: 8

Essa configuração proporcionou um desempenho estável e eficiente durante todas as fases dos testes, garantindo que o protótipo operasse em condições próximas às encontradas em ambientes reais de produção.

#### **Sistema Operacional:**

- Linux Ubuntu Focal Fossa 20.04.6 LTS

- Kernel Linux: 5.4.0-164-generic

A escolha do sistema operacional Linux Ubuntu foi motivada por sua estabilidade e suporte de longo prazo, proporcionando um ambiente confiável para a execução do protótipo.

#### **Ferramentas Utilizadas:**

- Docker: Versão 24.0.6 (compilação ed223bc)
- Docker-Compose: Versão 1.25.0
- Docker-py: Versão 4.1.0
- Python3: Versão 3.8.10

O uso do Docker simplificou a implantação e a gestão de contêineres, facilitando a replicação do ambiente em diferentes cenários. O Python3 foi empregado para desenvolver e integrar componentes específicos do COTTONTRUST.

#### **Repositório:**

- Repositório no GitHub: <https://github.com/mauriciopillon/cottontrust>

O código-fonte e a estrutura do COTTONTRUST estão disponíveis publicamente no GitHub, fornecendo transparência, colaboração e facilitando futuras contribuições à comunidade. Essas decisões de configuração e escolhas de ferramentas foram fundamentais para garantir a replicabilidade dos testes e a validade dos resultados obtidos.

## 5.2 PROTÓTIPO

O COTTONTRUST é experimentado e testado por meio de vários fluxos de trabalho envolvendo entidades da cadeia algodoeira que emitem e verificam credenciais. Uma visão geral do funcionamento do COTTONTRUST é explicada na Figura 22, usando as fases de A até G. Como visto na Seção 4.1, a arquitetura do COTTONTRUST incorpora três entidades claramente diferenciadas: o Emissor, o Titular e o Verificador, que neste cenário serão representados pelas entidades: UBA; Fardinho de Algodão e o Comprador do Mercado Internacional, respectivamente.

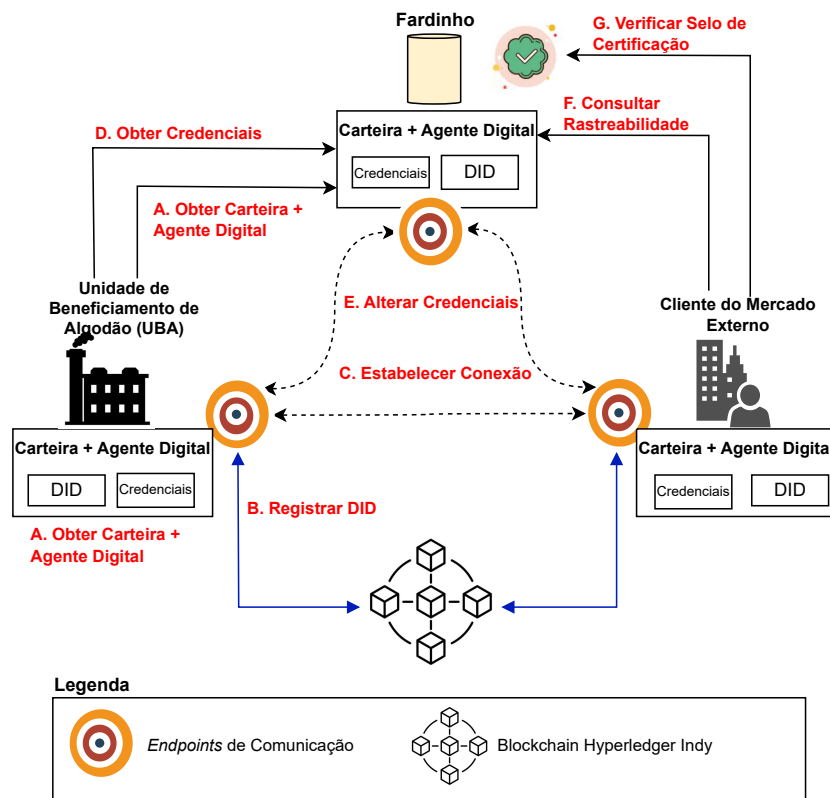


Figura 22 – Visão Geral do Funcionamento do COTTONTRUST

Cada uma dessas partes precisa de uma carteira e um agente digital para trocar informações com segurança entre elas, realizar operações criptográficas e armazenar dados privados, como chaves, DIDs e credenciais (fase A). Após essa etapa, as partes registram seus DIDs públicos, que as identificarão de forma globalmente única, por meio de seus agentes digitais, criando um registro imutável na blockchain. O documento DID, associado ao DID, também é armazenado na blockchain. O documento DID contém as chaves criptográficas, métodos de autenticação e outros metadados, que descrevem como se envolver em interações confiáveis com essa entidade (fase B).

Uma vez que as partes estão identificadas por meio de seus DIDs e possuem suas próprias carteiras e agentes digitais, a UBA irá produzir os Fardinhos de algodão em pluma. Ao produzir um Fardinho, a UBA obtém uma carteira e um agente digital para o mesmo, identificando-o de forma globalmente única utilizando um DID e registrando essa informação na blockchain (fases A e B para o Fardinho). O Fardinho, portanto, passa a ser uma entidade da cadeia. Todo DID possui um controlador DID, que provê controle sobre ele sem exigir permissão de qualquer outra parte e, no caso do Fardinho, a própria UBA será seu controlador nesse primeiro momento.

A fim de viabilizar qualquer transação entre duas entidades, é essencial, em

primeiro lugar, estabelecer uma conexão entre elas (fase C). Após estabelecida a conexão entre a UBA e o Fardinho, caberá à UBA gerar uma credencial verificável desse Fardinho, atestando sua legitimidade, privilégios de acesso e funções, que será enviada para a respectiva carteira digital (fase D).

Ao longo da jornada de um Fardinho de algodão, é plenamente possível que novas credenciais sejam adquiridas (como a credencial relacionada aos selos de certificação, exemplificadamente), outras sejam revogadas ou transferidas (fase E). Em qualquer tempo, entidades também podem obter informações de rastreabilidade (fase F), bem como é possível que uma entidade manifeste interesse em verificar a autenticidade dos selos de certificação à ele associados (fase G). Para fins de análise experimental, serão considerados os seguintes fluxos de trabalho, conforme:

1. **Transações do tipo CONNECT\_ENT:** A fim de viabilizar qualquer transação entre duas entidades no COTTONTRUST, é essencial, em primeiro lugar, estabelecer uma conexão entre elas. Para estabelecer essa conexão é imperativo que ambas tenham passado pelas fases A e B, garantindo a posse de suas carteiras, agentes digitais e DIDs, necessários para tal interação. A Figura 23 mostra as várias interações que cada entidade envolvida deverá executar nesse processo, supondo a conexão entre as entidades: UBA e Comprador do Mercado Internacional.
  - **UBA cria um convite de conexão:** a UBA, através de sua carteira digital, gera um QRCode chamado convite de conexão. Esse convite inclui informações sobre como o agente digital do Comprador do Mercado Internacional pode contatá-lo de maneira confiável por meio de um canal criptografado. Antes de gerar o QRCode, o agente de borda da UBA gera um *nonce* — *token* criptográfico gerado aleatoriamente — e o envia ao agente de nuvem da UBA para notificá-lo de que espera uma mensagem associada a esse *nonce*. O *nonce* está incluído no QRCode, tornando-o exclusivo para o Comprador do Mercado Internacional, de forma que, quando a UBA estabelecer sua próxima conexão com qualquer outra entidade o QRCode será diferente.
  - **Comprador do Mercado Internacional usa seu aplicativo da carteira digital para escanear o QRCode:** Assim que o agente de borda do Comprador do Mercado Internacional reconhece que este é um convite de conexão, ele instrui a carteira a gerar um novo par de chaves pública/privada e um DID baseado neste par de chaves. O DID identificará a conexão exclusiva do Comprador do Mercado Internacional com a UBA, de uma maneira que apenas os dois conhecem.

Depois que o par de chaves e o DID são salvos na carteira do Comprador do Mercado Internacional, seu agente de borda cria uma mensagem de solicitação de conexão que inclui um documento DID, preparado exclusivamente para a UBA. O documento DID inclui o novo DID, a chave pública correspondente e o endereço de rede do agente de nuvem do Comprador do Mercado Internacional (chamado de terminal de serviço).

O agente de borda do Comprador do Mercado Internacional envia sua mensagem de solicitação de conexão ao agente de nuvem do Comprador do Mercado Internacional com instruções para encaminhá-la ao agente de nuvem da UBA por meio do canal criptografado que este identificou em seu convite de conexão.

- **UBA responde a conexão:** O agente de nuvem da UBA recebe a mensagem do agente de nuvem do Comprador do Mercado Internacional e a envia para seu agente de borda, perguntando se a UBA deseja confirmar a conexão. a UBA confirma e seu agente de borda salva as informações de conexão do Comprador do Mercado Internacional em sua carteira.

Agora o agente de borda da UBA faz a mesma coisa que Comprador do Mercado Internacional fez: gera um novo par de chaves pública/privada exclusivo e um DID conhecido apenas pelo Comprador do Mercado Internacional. Salva-os em sua carteira e cria uma resposta de conexão que é a imagem espelhada da solicitação de conexão do Comprador do Mercado Internacional: contém o DID da UBA, a chave pública e os terminais de serviço para a conexão.

O agente de borda da UBA pode criptografar esta mensagem usando a chave pública do documento DID do Comprador do Mercado Internacional para que apenas Comprador do Mercado Internacional possa lê-la. Assim que estiver pronto, o agente de borda da UBA envia sua resposta de conexão para seu agente de nuvem com instruções para encaminhá-lo para o terminal de serviço privado que o agente do Comprador do Mercado Internacional forneceu a UBA.

- **Os agentes do Comprador do Mercado Internacional completam a conexão:** O agente de nuvem do Comprador do Mercado Internacional encaminha a resposta de conexão para o agente de borda, que salva o documento DID na carteira do Comprador do Mercado Internacional. O agente de borda notifica o Comprador do Mercado Internacional que a conexão está completa em ambas as direções.

## 2. **Transações do tipo REG\_ENTITY:** As entidades Unidade de Beneficiamento de Algodão (UBA), Fardinho de Algodão e Comprador do Mercado Internacional

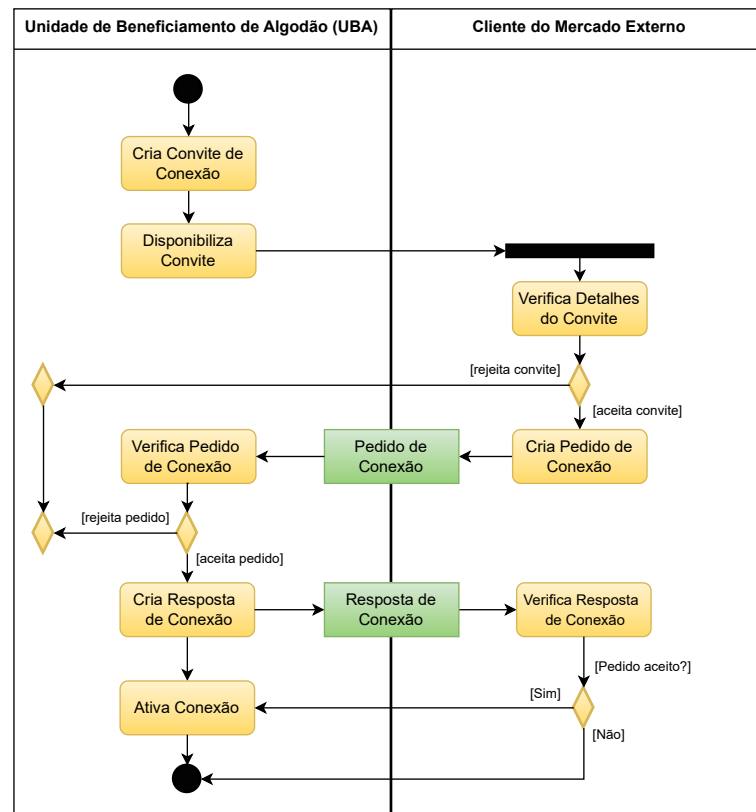


Figura 23 – Diagrama de atividade do estabelecimento de conexão entre duas entidades

efetuar seus registros de *Decentralized Identifiers* (DIDs) na blockchain. Após serem registrados, os DIDs são armazenados de forma privada nas carteiras digitais. Cada DID tem uma chave pública e uma chave privada associadas. A chave privada é armazenada na carteira digital, junto com o DID, enquanto a chave pública é armazenada na blockchain.

Dessa forma, uma vez que uma entidade da cadeia produtiva deseja integrar à blockchain, ela deve registrar seu DID público, logo após a criação da carteira digital. Para isso, a entidade primeiramente cria o DID por meio da sua carteira digital. Em seguida, prepara uma mensagem criptografada contendo o DID e a chave pública correspondente, e a envia para a blockchain. Caso haja consenso, o DID da entidade é registrado.

3. **Transações do tipo REG\_CREDENTIAL, REG\_SCHEMA e REG\_DEF:** Todas as partes envolvidas na cadeia têm um interesse mútuo em adquirir credenciais que lhes permitam realizar transações comerciais, tanto na compra quanto na venda de produtos. Essas credenciais abrangem diversos aspectos, como a obtenção de documentos oficiais, e.g., o Cadastro Nacional de Pessoa Jurídica (CNPJ) e o Registro de Exportadores e de Importadores (REI); bem como credenciais financeiras e outras relevantes para suas atividades comerciais. Essas

credenciais são emitidas pelas entidades responsáveis, tais como agências governamentais ou instituições financeiras, que têm a autoridade para conceder essas certificações legítimas.

Na Figura 24, a agência governamental é uma representação da organização responsável por registrar esquemas relacionados às credenciais das entidades da cadeia produtiva do algodão na blockchain, e.g., esquema "Commodity", esquema "Comprador do Mercado Internacional", esquema "UBA", e assim por diante (passo 1).

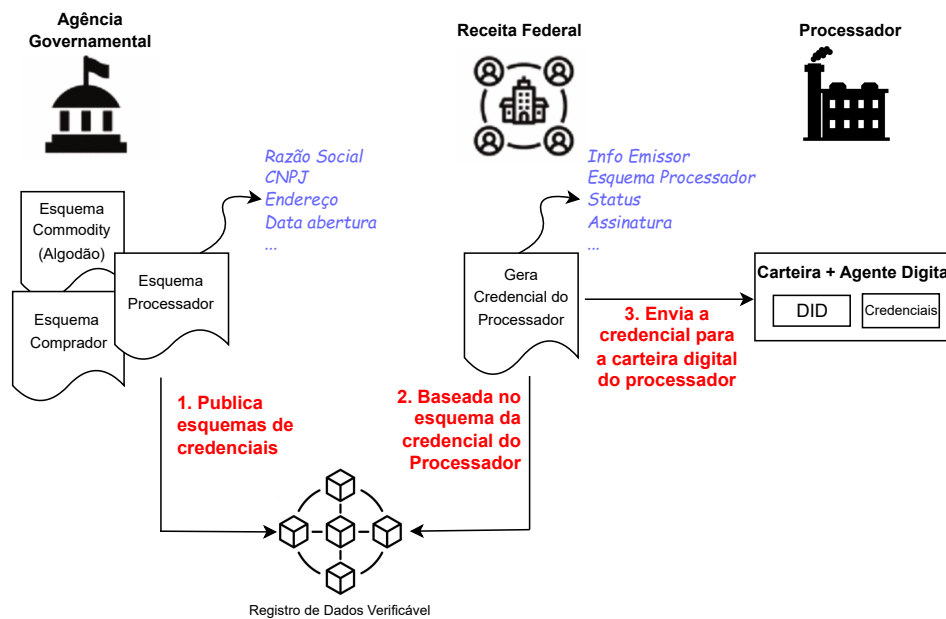


Figura 24 – Esquemas e Credenciais

No Brasil, toda empresa deve ter um registro chamado Cadastro Nacional de Pessoa Jurídica (CNPJ), junto ao Ministério da Fazenda (agência governamental) que é responsável por publicar o esquema da credencial do CNPJ das empresas na blockchain. A Receita Federal, no exercício de suas atribuições, ao registrar uma empresa utiliza-se do esquema da credencial (passo 2), para criar uma instância concreta de uma credencial para essa empresa específica. Em termos mais técnicos, a definição e geração da credencial é um objeto JSON que adere ao esquema da credencial, contendo os atributos específicos da credencial e os dados correspondentes e é enviada à carteira digital do Titular, neste caso a UBA (passo 3).

A UBA, depois de registrar seu DID na blockchain, estabelece uma conexão com a Receita Federal e solicita sua credencial relativa ao seu CNPJ. A Receita Federal emite a credencial da UBA após verificar a sua elegibilidade. Esse fluxo é demonstrado na Figura 25 .

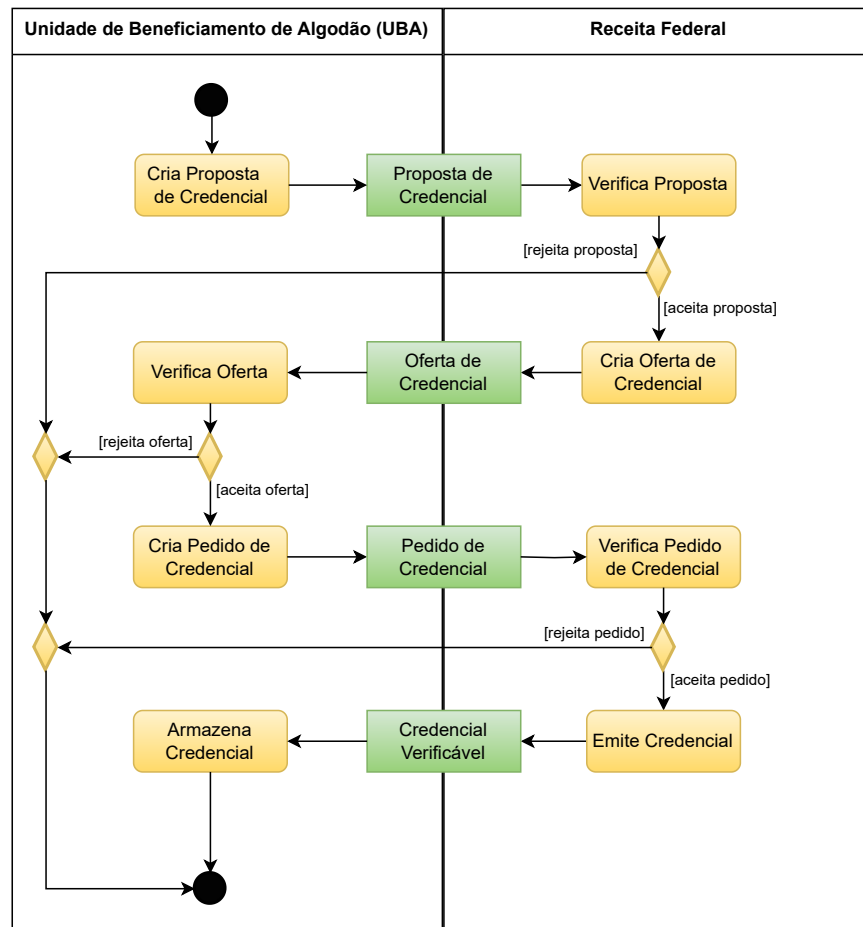


Figura 25 – Diagrama de atividade do processo de Obtenção de Credenciais

Reiterando, no transcorrer de sua existência, cada entidade é adquirida inúmeras credenciais verificáveis que atestam sua integridade e conformidade com normas específicas. No contexto específico do Fardinho, é pertinente ressaltar a obtenção de duas credenciais de especial relevância: a credencial do Laudo de Classificação e a credencial do Selo de Certificação.

A credencial do Laudo de Classificação constitui-se como um documento formal que atesta a qualidade e características intrínsecas do Fardinho de algodão, proporcionando informações detalhadas sobre sua classificação e conformidade com os padrões estabelecidos. Este laudo desempenha um papel crucial na validação das propriedades do produto, contribuindo para a confiança e transparência nas transações comerciais.

Por sua vez, a credencial do Selo de Certificação representa uma garantia adicional de autenticidade e conformidade. Este selo, emitido por entidades certificadoras reconhecidas, atesta que o Fardinho atende aos requisitos estipulados por normas e regulamentos específicos. A presença deste selo confere ao produto uma distinção que é de fundamental importância no mercado, assegurando aos

compradores a qualidade e procedência confiável do fardinho de algodão.

4. **Transações do tipo QUERY\_SEAL, QUERY\_COTTON e QUERY\_LAUDO:** Na Figura 26 é apresentado o diagrama de atividades que representa o processo de apresentação de provas. No contexto analisado, delinea-se o processo de verificação da legitimidade dos selos de certificação atribuídos a cada Fardinho de algodão. Nesse cenário, o Comprador do Mercado Internacional manifesta o interesse em verificar se o selo de certificação, alegadamente emitido por determinada entidade, é autêntico.

Diante desse desafio, após estabelecer uma conexão direta com o Fardinho em questão, o Comprador solicita à carteira digital do fardinho uma comprovação da autenticidade do selo em questão. O Fardinho possui uma credencial verificável que corresponde ao selo de certificação, e, nesse procedimento, é capaz de gerar apresentação verificável, *i.e.*, uma evidência concreta da autenticidade do selo, e apresentá-la ao Comprador. Este, munido das informações contidas na referida apresentação verificável, consegue efetuar uma verificação precisa, assegurando-se da autenticidade do selo de certificação. Este método de verificação confere ao Comprador do Mercado Internacional uma garantia substancial quanto à legitimidade dos produtos adquiridos, reforçando a confiança no sistema.

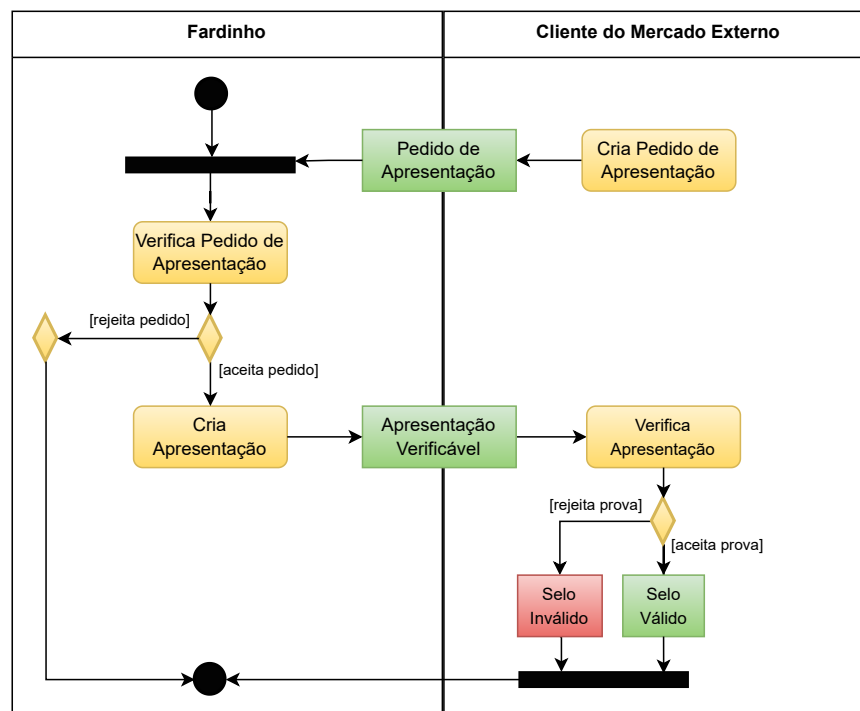


Figura 26 – Diagrama de atividade do processo de Apresentação e Verificação de Provas

Da mesma forma é o funcionamento do fluxo para verificação da autenticidade

dos Laudos de Classificação e obtenção das informações pertinentes à rastreabilidade.

5. **Transações do tipo SELL\_COTTON e PROOF\_VERIFY:** Este fluxo representa a simulação de 10.000 vendas de Fardinhos de Algodão pela UBA, para compradores do mercado internacional. A UBA é responsável pela produção dos Fardinhos de algodão e pelo seu registro na cadeia. Conforme mencionado anteriormente, a UBA cria um DID, adquire uma carteira digital e gera uma credencial verificável para o Fardinho. Por sua vez, o Comprador do Mercado Internacional desempenha o papel de verificar as informações relacionadas ao Fardinho, conferindo se a classificação foi realizada por um classificador qualificado, e a veracidade das alegações de qualidade. Além disso, o Comprador do Mercado Internacional tem a capacidade de rastrear todo o histórico do fardo (fase F) e verificar a autenticidade dos selos de certificação associados a ele (fase G).

Ao concordar com as condições estabelecidas e comprovar o pagamento do produto, o controlador do DID do Fardinho é transferido para o Comprador do Mercado Internacional, tornando-o o legítimo proprietário da mercadoria.

Para este cenários, considera-se:

- Comprador do Mercado Internacional e UBA já se conhecem e possuem uma conexão.
- Comprador do Mercado Internacional e UBA já possuem conexões e credenciais com seus bancos.
- O Comprador do Mercado Internacional esteja interessado em comprar fardinhos de algodão em pluma da UBA, e portanto já fez contato e negociou as condições comerciais.

Na sequência são enumerados os passos para essa transação:

- O Comprador do Mercado Internacional possui uma credencial de autorização de pagamento de seu banco, que ele utilizará para pagar a UBA.
- O Comprador do Mercado Internacional conclui a compra do algodão e, neste caso, envia o comprovante de sua credencial de Autorização de Pagamento para a UBA.
- O Comprador do Mercado Internacional recebe sua credencial de Recibo de Compra da UBA e o controlador DID dos Fardinhos para a ser o DID do Comprador do Mercado Internacional.

### 5.3 PLANO DE TESTES

Na avaliação de desempenho do protótipo, adotamos o tempo total de transação como a métrica principal para medir a eficiência nas transações REG\_ENTITY e SELL\_COTTON, que foram escolhidas para estabelecer as medições, visto que a REG\_ENTITY representa as transações que efetuam gravação na blockchain e a SELL\_COTTON representa as transações que apenas consultam a blockchain. Essa escolha está fundamentada na importância crítica desses processos para a funcionalidade geral da plataforma. Os testes têm como objetivo avaliar a escalabilidade do sistema e seu comportamento sob diferentes cargas de transação, com resultados esperados para obter *insights* sobre a eficiência, escalabilidade e capacidade do sistema COTTONTRUST em gerenciar efetivamente seus recursos. Esses dados são essenciais para otimização e validação em vários contextos operacionais. Todos os resultados são calculados com base na média de 10 execuções.

#### **Operações Modeladas:**

- REG\_ENTITY: Este cenário experimental compreende a execução das seguintes operações: (i) Registro de entidades UBA, Fardinho de Algodão e Comprador do Mercado Internacional. (ii) Criação de 100 entidades de cada tipo. (iii) Identificação e registro na blockchain por DID, com respectivas carteiras digitais.
- SELL\_COTTON: Este cenário representa a simulação de 10.000 vendas de fardos de algodão pela UBA para compradores do mercado internacional.

#### **Cenário de Teste:**

- Variação de Nós na blockchain: a aplicação é hospedada por 4, 8, 16 e 32 nós na blockchain. Para cada cenário, consideramos o tempo total médio de transação para as transações REG\_ENTITY e SELL\_COTTON.

### 5.4 DISCUSSÃO E ANÁLISE DE RESULTADOS

Inicialmente, o Tempo Total de Transação para o tipo REG\_ENTITY (Figura 27), resumido pelo número de nós na blockchain, indicou uma variação no tempo de transação conforme o número de nós aumenta. Apesar dos resultados para 4 e 8 nós se mostrarem estáveis, com tempos de transação consistentes em torno de 3 segundos, o leve aumento no tempo de transação ao passar de 8 para 16 nós pode indicar um ponto de transição cujo a complexidade da rede começa a impactar marginalmente o desempenho.

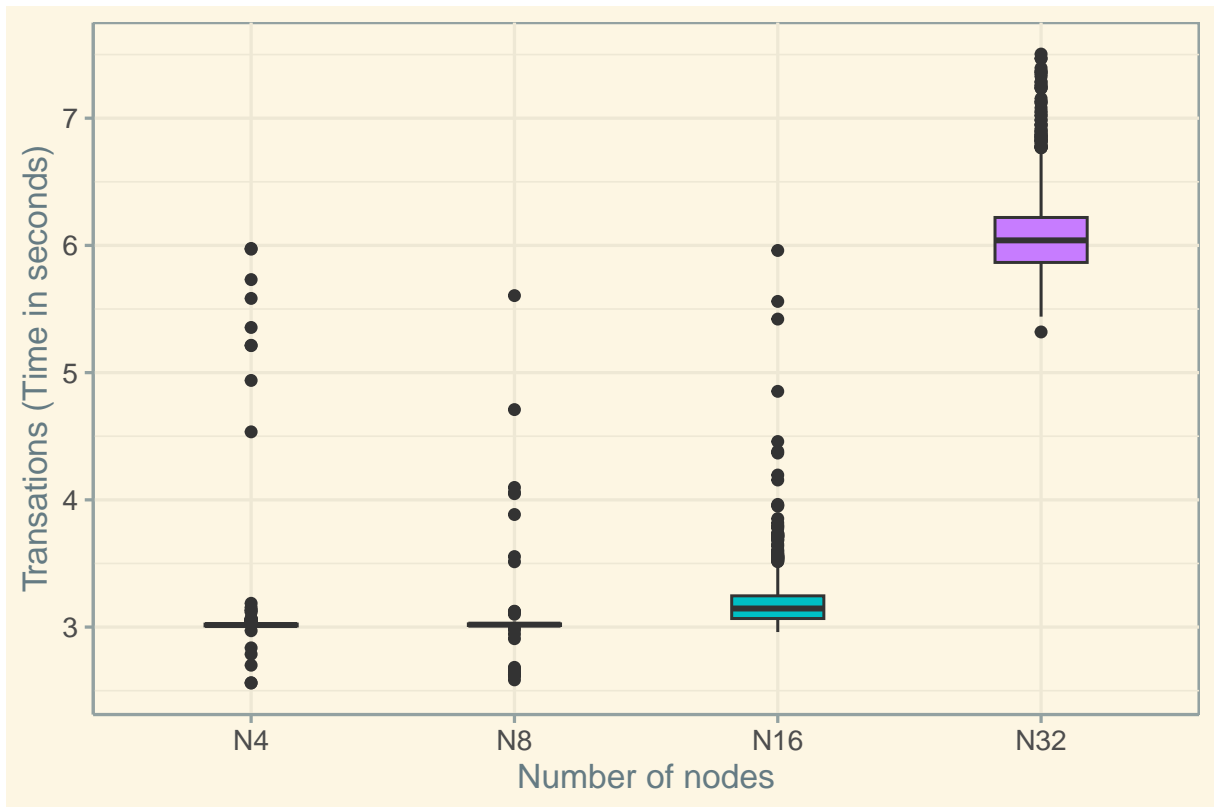


Figura 27 – Transações do tipo REG\_ENTITY

Ao expandir de 16 para 32 nós, observa-se um aumento no tempo de transação, sugerindo uma potencial influência do aumento da complexidade da rede. O aumento no tempo médio de transação à medida que o número de nós na blockchain aumenta é um comportamento parcialmente esperado em sistemas distribuídos. Essa tendência está relacionada à necessidade de consenso entre os nós para validar e registrar transações no livro-razão compartilhado, porque, à medida que o número de nós aumenta, a complexidade do consenso também aumenta, já que mais entidades precisam concordar sobre a validade das transações.

A Figura 28 resume o Tempo Total de Transação para SELL\_COTTON em relação ao número de nós na blockchain. Os resultados mostram tempos de transação muito semelhantes, indicando uma estabilidade ou eficiência relativamente constante, com um leve aumento no tempo de transação com 32 nós. As transações SELL\_COTTON têm tempos significativamente menores em comparação com as transações REG\_ENTITY. As transações REG\_ENTITY, envolvendo consenso na blockchain e registro no livro-razão, têm tempos de processamento intrinsecamente mais altos. As transações SELL\_COTTON, principalmente consultas, têm tempos menores, pois não envolvem consenso para atualizar o livro-razão. A diferença observada está alinhada com as expectativas, dada a natureza das transações. É comum que operações intensivas em gravação (como REG\_ENTITY) levem mais tempo devido ao mecanismo de consenso e à atualização do livro-razão.

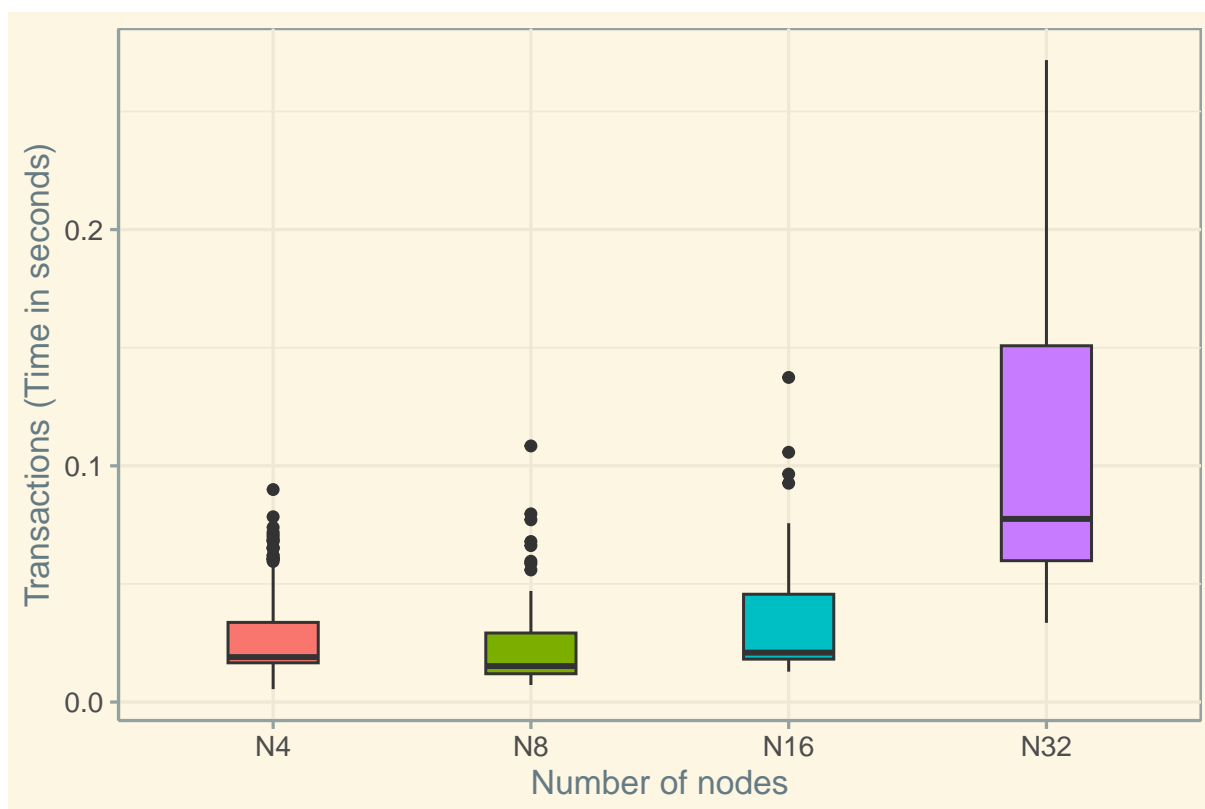


Figura 28 – Transações do tipo SELL\_COTTON

## 5.5 CONSIDERAÇÕES PARCIAIS

Os experimentos conduzidos foram direcionados para os processos de registro de entidades (transações REG\_ENTITY) e transações de venda de algodão (transações SELL\_COTTON), com ênfase na avaliação da escalabilidade e eficiência do COTTONTRUST. Em ambas as instâncias, os resultados evidenciaram uma correlação direta entre o aumento no número de transações e o número de nós na blockchain. Esta constatação instiga reflexões pertinentes acerca da otimização do desempenho do sistema em ambientes que contam com um maior número de nós.

As variações nos tempos de transação indicam a necessidade de uma análise sobre o impacto do tamanho da rede na eficácia do COTTONTRUST. As etapas subsequentes devem englobar uma análise mais aprofundada dessas variações, possivelmente explorando técnicas de otimização para preservar a eficiência, mesmo em contextos mais complexos. Em conclusão parcial, os resultados até o momento ratificam a relevância do COTTONTRUST na cadeia produtiva do algodão. Contudo, a análise dos experimentos denota a contínua necessidade de aprimoramento e adaptação do sistema para enfrentar os desafios inerentes à sua implementação em escalas mais abrangentes.

## 6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Atualmente, os atributos que caracterizam as identidades digitais estão nas mãos de terceiros, que são externos à entidade a que se referem. O modelo de gerenciamento de identidades SSI nasceu da necessidade da entidade possuir o controle total das suas identidades pessoais e da proteção dos dados associados, podendo gerenciar seus atributos de forma independente, decidindo quais compartilhar e com quem. Os atributos, se a entidade permitir, podem ser verificados em tempo real e a qualquer momento por qualquer outra entidade que tenha interesse. Isso permite a redução de 'apertos de mão' em diferentes níveis e economiza custos e tempo que, de outra forma, seriam necessários ao usar serviços de terceiros para verificação de informações. As vantagens de recorrer à uma arquitetura SSI, como o aumento de privacidade e segurança dos dados privados dos seus utilizadores, e a remoção da responsabilidade e dos custos que uma empresa é obrigada a despende para manter esses dados, fizeram com que este tema ganhasse bastante notoriedade.

Com base nos princípios do SSI, neste trabalho é apresentado o COTTON-TRUST, um sistema autossobrano, transparente e descentralizado, para obter rastreabilidade do Fardinho do algodão, bem como fornecer recursos de verificabilidade dos respectivos selos de certificação. O sistema objetiva mitigar as preocupações acerca da confiança, rastreabilidade e verificabilidade, inerentes à cadeia de produção do algodão, devido à sua natureza complexa, diversa e geograficamente dispersa. Deste modo, integra uma blockchain e carteiras digitais criptograficamente seguras, ambas desenvolvidas utilizando Hyperledger Indy.

No COTTONTRUST, nenhum dado pessoal é armazenado na blockchain, assim, a conformidade com os objetivos fundamentais da LGPD e GDPR pôde ser alcançada. Além disso, as interações entre as entidades não são rastreáveis e não dependem de terceiros, pois uma entidade Verificadora não precisa entrar em contato diretamente com a Emissora durante o processo de verificação das informações.

Por outro lado, a autenticidade das informações pode ser verificada digitalmente em segundos, *i.e.*, como as credenciais são verificáveis criptograficamente em tempo real, isso também melhora a experiência do usuário. Outro benefício relacionado à descentralização, é que as entidades usam carteiras digitais para gerenciar suas chaves e dados privados, ao contrário dos sistemas típicos que armazenam dados de forma centralizada. Isso propicia controle total sobre seus dados pessoais, evitando a criação de um armazenamento de dados centralizado que pode ser alvo para *hackers*.

Por fim, o método descentralizado de processamento das informações torna o processo transparente. Como o COTTONTRUST é baseado em protocolos e ferramentas de desenvolvimento de código aberto, ele oferece mais flexibilidade para examinar como funciona e se existem brechas que devem ser observadas. Além disso, permite que qualquer pessoa examine como diferentes componentes operam, tornando o sistema geral transparente e confiável.

### Trabalhos Futuros

Como uma direção futura de desenvolvimento, é crucial realizar testes de usabilidade para colher a opinião dos usuários e, potencialmente, aprimorar, eliminar ou adicionar funcionalidades baseadas nessa análise. No que tange as credenciais verificáveis, a implementação e tratamento da possibilidade de revogação das credenciais também é assunto para trabalhos futuros.

A utilização de outros cenários de testes também são um propósito para pesquisas futuras, bem como os mecanismos de governança relativos à aceitação legal da proposta deixam algumas questões em aberto. Pesquisas futuras poderiam explorar a utilização de outras tecnologias de comunicação para atender situações sem uma conexão garantida à Internet. Além disso, no lugar dos DIDs, *Non-fungible tokens* (NFT) poderiam ser utilizados como alternativa para identificar unicamente as entidades.

## 6.1 PRODUÇÕES

As seguintes publicações foram fruto deste trabalho:

- Aceita (retirada do evento): **DOCTRUST: Plataforma Autossobrerana para Autenticação e Verificação de Documentos Digitais** - XXIII Escola Regional de Alto Desempenho da Região Sul (ERAD/RS 2023). Maio/2023. (Impossibilidade de ir ao evento)
- Publicada: **Sistema de Unidade de Beneficiamento de Algodão (UBA) modelado em Identidade Autossobrerana** - 20ª Escola Regional de Redes de Computadores (ERRC). Outubro/2023. (*Best Paper*)
- Aceita (aguardando publicação): **COTTONTRUST: Reliability and Traceability in Cotton Supply Chain Using Self-Sovereign Identity** - 38th International Conference on Advanced Information Networking and Applications - AINA. Abril/2024.
- Aceita (aguardando publicação): **COTTONTRUST: Análise dos Tempos de Criação de Entidades com Base em Identidades Autossobreranas** - XXIII Escola Regional de Alto Desempenho da Região Sul (ERAD 2024). Março/2024.

Este trabalho também gerou a proposta de três IC - Iniciação Científica, coordenados pela mestranda:

- IC 2022-2023: "**Hyperledger Indy: Revolucionando a Identidade Digital**" - Gabriel Felipe Cordeiro da Silva (TADS)
- IC 2023-2024: "**CottonTrust: Agro 4.0 com Identidades Distribuídas para Rastreamento da Produção.**" - Gabriel Felipe Cordeiro da Silva (TADS)
- IC 2023-2024: "**Aplicando Hyperledger ao Agro 4.0**" - Gilson Sohn Junior (BCC)

## REFERÊNCIAS

- ABRAMSON, W. **CL Signatures for Anony-mous Credentials**. 2019. Url: <https://misterwip.uk/cl-signatures>.
- AGRAWAL, T. K. et al. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. **Computers & Industrial Engineering**, v. 154, p. 107130, 2021. ISSN 0360-8352. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0360835221000346>>.
- ALLEN, C. The path to self-sovereign identity. **Life With Alacrity**, 2016. Disponível em: <<http://lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>>.
- AMIPA, A. M. dos Produtores de A. **Beneficiamento**. 2023. Url: <https://amipa.com.br/ben-algodoeiras>.
- ARIES, H. 2022. Url: <https://www.hyperledger.org/use/aries>.
- AUBLIN, P.-L. et al. The next 700 bft protocols. **ACM Transactions on Computer Systems (TOCS)**, ACM New York, NY, USA, v. 32, n. 4, p. 1–45, 2015.
- AUBLIN, P.-L.; MOKHTAR, S. B.; QUÉMA, V. Rbft: Redundant byzantine fault tolerance. In: IEEE. **2013 IEEE 33rd international conference on distributed computing systems**. [S.l.], 2013. p. 297–306.
- BHARGAV-SPANTZEL, A. et al. User centricity: a taxonomy and open issues. **Journal of Computer Security**, IOS Press, v. 15, n. 5, p. 493–527, 2007.
- BHATTACHARYA, M. P.; ZAVARSKY, P.; BUTAKOV, S. Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain. p. 1–7, 2020.
- BUAINAIN, A. M. et al. **Cadeia produtiva do algodão**. [S.l.]: Bib. Orton IICA/CATIE, 2007. v. 4.
- BUTERIN, V. On public and private blockchains. **Ethereum blog**, v. 7, n. 1, 2015.
- CAMERON, K. **The Laws of Identity**. 2005. Disponível em: <<https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>>. Acesso em: 08 maio 2022.
- CHOPRA, S.; MEINDL, P. Strategy, planning, and operation. **Supply Chain Management**, Pearson New York, NY, USA, p. 13–17, 2001.
- COCCO, L.; TONELLI, R.; MARCHESI, M. Blockchain and self sovereign identity to support quality in the food supply chain. **Future Internet**, Multidisciplinary Digital Publishing Institute, v. 13, n. 12, p. 301, 2021.
- COMMITTEE, I. C. A. **World Cotton Statistics Report**. 2023. Disponível em: <[https://icac.shinyapps.io/ICAC\\_Open\\_Data\\_Dashbooard/#](https://icac.shinyapps.io/ICAC_Open_Data_Dashbooard/#)>. Acesso em: 07 junho 2023.
- CONCEIÇÃO, J. C. P. R. d.; BARROS, A. L. M. d. Certificação e rastreabilidade no agronegócio: instrumentos cada vez mais necessários. Instituto de Pesquisa Econômica Aplicada (Ipea), 2005.

COSTA, A. C. R. d.; ROCHA, É. R. P. d. Panorama da cadeia produtiva têxtil e de confecções e a questão da inovação. Banco Nacional de Desenvolvimento Econômico e Social, 2009.

ČUČKO, Š.; TURKANOVIC, M. Decentralized and self-sovereign identity: Systematic mapping study. **IEEE Access**, IEEE, v. 9, p. 139009–139027, 2021.

DAVIE, M. et al. The trust over ip stack. **IEEE Communications Standards Magazine**, IEEE, v. 3, n. 4, p. 46–51, 2019.

DIF, D. I. F. **DIDComm Messaging V2**, [online]. 2022. Url: <https://github.com/decentralized-identity/didcomm-messaging>.

DIF, D. I. F. **Secure Data Storage**, [online]. 2022. Url: <https://identity.foundation/working-groups/secure-data-storage.html>.

ETHEREUM. **Ethereum**. 2023. Url: <https://ethereum.org/pt-br/>.

FERDOUS, M. S.; CHOWDHURY, F.; ALASSAFI, M. O. In search of self-sovereign identity leveraging blockchain technology. **IEEE Access**, IEEE, v. 7, p. 103059–103079, 2019.

FERREIRA, B. N. et al. Cadeia produtiva do algodão no brasil. **Research, Society and Development**, v. 11, n. 10, p. e298111031730–e298111031730, 2022.

FOUNDATION, L. 2023. Url: <https://www.linuxfoundation.org/>.

GALVÃO, T. F.; PANSANI, T. d. S. A.; HARRAD, D. Principais itens para relatar revisões sistemáticas e meta-análises: A recomendação prisma. **Epidemiologia e serviços de saúde**, SciELO Public Health, v. 24, p. 335–342, 2015.

GOLDREICH, O.; MICALI, S.; WIGDERSON, A. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. **Journal of the ACM (JACM)**, ACM New York, NY, USA, v. 38, n. 3, p. 690–728, 1991.

GRASSI, P. A.; GARCIA, M. E.; FENTON, J. L. **Digital Identity Guidelines**. 2017. Disponível em: <<https://doi.org/10.6028/NIST.SP.800-63-3>>. Acesso em: 08 maio 2022.

GRIGG, I. Triple entry accounting. **Systemics Inc**, p. 1–10, 2005.

GRUNERT, K. G.; HIEKE, S.; WILLS, J. Sustainability labels on food products: Consumer motivation, understanding and use. **Food policy**, Elsevier, v. 44, p. 177–189, 2014.

HADER, M. et al. Applying integrated blockchain and big data technologies to improve supply chain traceability and information sharing in the textile sector. **Journal of Industrial Information Integration**, v. 28, p. 100345, 2022. ISSN 2452-414X. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S2452414X22000176>>.

HARDMAN, D. **Aries RFC 0015: ACKs**. 2021. Url: <https://github.com/hyperledger/aries-rfcs/blob/main/features/0015-acks/README.md>.

HIRSCH, F.; PHILPOTT, R.; MALER, E. **Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0**. 2004.

INDY, H. 2022. Url: <https://www.hyperledger.org/use/hyperledger-indy>.

ITU, U. I. de T. [S.I.]: União Internacional de Telecomunicações - ITU, 2009. Disponível em: <<https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2720>>. Acesso em: 07 maio 2022.

ITU, U. I. de T. **Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions**. 2019. Disponível em: <<https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>. Acesso em 11/11/2022>.

ITU, U. I. de T. 2022. Disponível em: <<https://www.itu.int>>. Acesso em: 07 maio 2022.

JOSANG, A.; ALZOMAI, M.; SURIADI, S. Usability and privacy in identity management architectures. p. 143–152, 2007.

JOSANG, A. et al. Trust requirements in identity management. **Conferences in Research and Practice in Information Technology Series**, v. 44, p. 99–108, 01 2005.

JOSANG, A.; POPE, S. User centric identity management. v. 22, p. 2005, 2005.

JOSEPH, M. **Quality Planning and Analysis: From Product Development Through Usage**. [S.I.]: McGraw-Hill, 2001.

KHATEEV, N. **Aries RFC 0036: Issue Credential Protocol 1.0**. 2019. Url: <https://github.com/hyperledger/aries-rfcs/blob/main/features/0036-issue-credential/README.md>.

KHATEEV, N. **Aries RFC 0037: Present Proof Protocol 1.0**. 2019. Url: <https://github.com/hyperledger/aries-rfcs/blob/main/features/0037-present-proof/README.md>.

LOFFRETO, D. **What is ‘Sovereign Source Authority’?** 2012. Disponível em: <<http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html>>. Acesso em: 09 julho 2022.

LÓPEZ, M. A. Self-sovereign identity: The future of identity: Self-sovereignty, digital wallets, and blockchain. **Inter-American Development Bank**, v. 10, p. 0002635, 2020.

LUNDKVIST, C. et al. Uport: A platform for self-sovereign identity. 2017. **Cited on**, p. 4, 2019. Disponível em: <[http://blockchainlab.com/pdf/uPort\\_whitepaper\\_DRAFT20161020.pdf](http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf)>.

MALIK, S. et al. Tradechain: Decoupling traceability and identity in blockchain enabled supply chains. In: IEEE. **2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)**. [S.I.], 2021. p. 1141–1152.

MARINO, F. et al. Finid. **Revista LIFT papers**, v. 2, n. 2, 2019.

MCKNIGHT, D. H.; CHERVANY, N. L. The meanings of trust. Citeseer, 1996.

MEIRA, A. C. B. T. Linkedid: Uma abordagem baseada em um manifesto autocontido e verificável para associação entre identidades digitais centralizadas e descentralizadas. In: . [S.I.: s.n.], 2022.

MICHAELIS, M.; MICHAELIS, H. **Dicionário brasileiro da língua portuguesa**. [S.l.: s.n.], 2021.

NAIK, N.; JENKINS, P. uport open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain. p. 1–7, 2020.

NAKAMURA, E. T. et al. Identidade digital descentralizada: Conceitos, aplicações, iniciativas, plataforma de desenvolvimento e implementação de caso de uso. **Sociedade Brasileira de Computação**, 2019.

NEVES, M. F.; PINTO, M. J. A. A cadeia do algodão brasileiro: safra 2016/2017: desafios e estratégias. **ABRAPA—Associação Brasileira dos Produtores de Algodão**, 2017.

NODE, I. 2023. Url: <https://hyperledger-indy.readthedocs.io/projects/node/en/latest/index.html>.

PEIXOTO, R. J. M. **DIDs, Claims, Credentials e Blockchains (Self-sovereign Identity)**. Tese (Doutorado) — Universidade do Minho, 2021.

PINHO, J. B. **Publicidade e vendas na Internet: técnicas e estratégias**. São Paulo: Summus Editorial, 2000. ISBN 9788532307460.

PLENUM, I. 2023. Url: <https://hyperledger-indy.readthedocs.io/projects/plenum/en/latest/index.html>.

PREUKSCHAT, A.; REED, D. **Self-sovereign identity**. [S.l.]: Manning Publications, 2021.

REACT.JS, J. **React.JS**. 2023. Url: <https://pt-br.react.dev/blog/2023/03/16/introducing-react-dev>.

REED, D.; LAW, J.; HARDMAN, D. The technical foundations of sovryn. a white paper from the sovryn foundation (2016). 2019. Disponível em: <<https://www.evernym.com/wp-content/uploads/2017/07/The-TechnicalFoundations-of-Sovryn.pdf>>.

RICOEUR, P. **Tempo e Narrativa - Tomo III**. Campinas, SP, Brasil: Papyrus, 1997.

SCHARDONG, F.; CUSTÓDIO, R. Self-sovereign identity: A systematic map and review. **arXiv preprint arXiv:2108.08338**, 2021.

SDK, I. 2023. Url: <https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/index.html>.

SEZER, B. B.; TOPAL, S.; NURIYEV, U. Tppsupply : A traceable and privacy-preserving blockchain system architecture for the supply chain. **Journal of Information Security and Applications**, v. 66, p. 103116, 2022. ISSN 2214-2126. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S2214212622000096>>.

SHOCARD. **ShoCard White Paper**. 2019. Url: <https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf>.

SHUAIB, M. et al. Self-sovereign identity solution for blockchain-based land registry system: a comparison. **Mobile Information Systems**, Hindawi, v. 2022, 2022.

SIQUEIRA, A.; CONCEIÇÃO, A. F. da; ROCHA, V. Blockchain e identidades digitais descentralizadas: Fundamentos e oportunidades.

SMITH, S. M. Key event receipt infrastructure (keri). **arXiv preprint arXiv:1907.02143**, 2019.

SOARES, P. R. et al. Cadeia produtiva têxtil do algodão: globalização e competitividade. Universidade Federal Rural do Rio de Janeiro, 2010.

SOLTANI, R.; NGUYEN, U. T.; AN, A. A new approach to client onboarding using self-sovereign identity and distributed ledger. p. 1129–1136, 2018.

SOLTANI, R.; NGUYEN, U. T.; AN, A. A survey of self-sovereign identity ecosystem. **Security and Communication Networks**, v. 2021, 2021. Disponível em: <<https://doi.org/10.1155/2021/8873429>>.

SPORNY, M.; LONGLEY, D.; CHADWICK, D. **Verifiable Credentials Data Model v1.1**. [S.I.]: W3C, 2022. Disponível em: <<https://www.w3.org/TR/vc-data-model/>>. Acesso em: 04 junho 2022.

SPORNY, M. et al. **Decentralized Identifiers (DIDs) v1.0**. [S.I.]: W3C, 2021. Disponível em: <<https://www.w3.org/TR/did-core/>>. Acesso em: 20 maio 2022.

SPORNY, M. et al. **Decentralized Identifiers (DIDs) v1.0 - Methods**. [S.I.]: W3C, 2022. Disponível em: <<https://w3c.github.io/did-core/#methods>>. Acesso em: 20 janeiro 2023.

STROHMINGER, N.; KNOBE, J.; NEWMAN, G. The true self: A psychological concept distinct from the self. **Perspectives on Psychological Science**, v. 12, n. 4, p. 551–560, 2017. PMID: 28671854. Disponível em: <<https://doi.org/10.1177/1745691616689495>>.

STRÜCKER, J. et al. Self-sovereign identity: Foundations, applications, and potentials of portable digital identities. 2021.

TECHNOLOGIES, C. **CIVIC White Paper**. 2017. Url: <https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf>.

TOBIN, A. Sovrin: What goes on the ledger? **Sovrin Foundation**, p. 1–10, 2017.

TOBIN, A.; REED, D. The inevitable rise of self-sovereign identity: A white paper from the sovrin foundation [white paper]. **Sovrin. Org**, v. 23, 2017.

URSA, H. 2022. Url: <https://www.hyperledger.org/use/ursa>.

W3C, W. W. W. C. 2022. Disponível em: <<https://www.w3.org/>>. Acesso em: 07 maio 2022.

WEST, R. et al. **0160: Connection Protocol**. 2019. Url: <https://github.com/hyperledger/aries-rfcs/blob/main/features/0160-connection-protocol/README.md>.

WOLFF, B.; HENRIQUES, M. Estudo experimental sobre gestão de identidades autossobranas para avaliação de riscos e oportunidades de adoção pela rnp. In: **Anais do XXI SBSeg-Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, WGID-Workshop de Gestão de Identidades Digitais**. [S.I.: s.n.], 2021.

YAGA, D. et al. Blockchain technology overview. **arXiv preprint arXiv:1906.11078**, 2019.

ZAEEM, R. N. et al. Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study. p. 128–135, 2021.

## ANEXO A – IDENTIDADES DIGITAIS

O conceito de identidade está relacionado ao ambiente na qual esta será empregada, aos contextos semânticos e aos casos de uso. Dessa forma, para o dicionário, identidade pode ser entendida como uma série de características próprias de uma pessoa ou coisa por meio das quais podemos distingui-las (MICHAELIS; MICHAELIS, 2021); o filósofo francês Paul Ricoeur, por sua vez, escreve a respeito da distinção entre a identidade no sentido de igual, o mesmo, a qual é nomeada de *mesmice (idem)*, e a identidade no sentido de mutável, variável, chamada *ipseidade (ipse)* (RICOEUR, 1997). Na psicologia, o termo é geralmente referido a todos os traços psicológicos de uma pessoa, incluindo crenças, personalidade, e outros atributos (STROHMINGER; KNOBE; NEWMAN, 2017).

Para o propósito deste trabalho, será utilizada a definição da *International Telecommunication Union (ITU)* que considera a identidade uma representação de uma entidade, suficiente para identificá-la em um contexto particular. Uma entidade, por sua vez, é qualquer coisa existente no mundo real, incluindo indivíduos, organizações e coisas (ITU, 2022).

De acordo com a recomendação ITU-T Y.2720 (ITU, 2009) do *Telecommunication Standardization Sector (ITU-T)*, uma identidade consiste de:

- **Identificador:** conjunto de dígitos, caracteres e símbolos ou qualquer outra forma de dados usada para identificar unicamente uma identidade.
- **Credenciais:** atestado de qualificação, competência ou autoridade, expedida por terceiros com autoridade relevante ou competência para tal ato e que atesta a veracidade da identidade.
- **Atributos:** um conjunto de dados que descreve as características fundamentais de uma identidade.

Com a adição da palavra 'digital', o *National Institute of Standards and Technology (NIST)* define identidade digital como a representação única de um sujeito envolvido em uma transação online. Uma identidade digital é sempre única no contexto dos serviços digitais, mas não precisa necessariamente identificar exclusivamente o sujeito em todos os contextos (GRASSI; GARCIA; FENTON, 2017).

Kim Cameron, por sua vez, em seu artigo "*The Laws of Identity*" (CAMERON, 2005), especifica que uma identidade digital pode ser entendida como um conjunto de afirmações feitas por um sujeito digital sobre si mesmo ou outro assunto digital, e

descreve sete elementos essenciais (leis) que explicam os sucessos e fracassos de sistemas de identidade digital, conforme:

1. Os usuários devem estar no controle de como suas informações de identidade são compartilhadas.
2. A quantidade de informação divulgada só deve ser a mínima necessária exigida, e os dados não devem ser mantidos por mais tempo do que o necessário pelas outras entidades.
3. O usuário deve estar bem informado sobre quais entidades gerenciam suas informações de identidade.
4. As informações do usuário não devem ser criadas ou expostas de forma a permitir a correlação de dados, reconhecimento de padrões ou identificação de entidades por outras entidades.
5. Interoperabilidade e integração perfeita entre várias entidades suportadas por diferentes arquiteturas deve ser possível.
6. Integração confiável e segura entre usuários humanos e as máquinas devem ser habilitadas.
7. Experiência de usuário consistente em vários contextos e tecnologias.

Idealmente uma identidade digital deve ser criada através de um conjunto de atributos que permitam diferenciar uma entidade da outra, garantindo sua identificação única (MEIRA, 2022). Porém, para autenticar, autorizar e gerenciar dados de identidades, bem como permitir seu uso em transações digitais, faz-se necessário mecanismos de controle e de segurança adicionais, incluindo a gerência do ciclo de vida da utilização de identidades em aplicações computacionais. Dessa forma, para lidar de forma padronizada com as demandas de controle de autenticação e autorização de operações para usuários, foi introduzido o conceito de *Identity Management* (IdM) (ITU, 2009).

## A.1 GERENCIAMENTO DE IDENTIDADE

Quase 30 anos se passaram desde que Peter Steiner mostrou ao mundo pela primeira vez que “Na Internet, ninguém sabe que você é um cachorro”, um adágio sobre o anonimato da Internet publicado pela *The New Yorker* em 5 de julho de 1993 (PINHO, 2000). No entanto, esse famoso *cartoon* ainda continua atual e válido, pois representa o desafio de identificar pessoas online. Nesse contexto, o gerenciamento de identidades ainda conta com o que Kim Cameron (CAMERON, 2005) descreveu

como "uma colcha de retalhos de identidades únicas", compreendendo vários tipos de sistemas que não interagem entre si.

Um sistema de *Identity Management* consiste de uma coleção de ferramentas, processos e políticas usadas para gerenciar identidades, sua autenticação, autorização, funções e privilégios, proporcionando segurança nas aplicações (ITU, 2009).

Diferentes modelos de gerenciamento de identidade possuem diferentes requisitos de confiança. Existe uma variedade de definições de confiança, muitas das quais dependem do contexto em que a interação ocorre. McKnight e Chervany (1996) definem confiança da seguinte forma:

"Confiança é a medida em que uma parte está disposta a depender de algo ou alguém em uma determinada situação com um sentimento de relativa segurança, ainda que consequências negativas possam acontecer"(MCKNIGHT; CHERVANY, 1996).

Embora relativamente geral, esta definição inclui implicitamente os requisitos básicos da confiança que são: 1) dependência da parte confiável; 2) confiabilidade do parte confiável; e 3) risco caso a parte confiável não executar como esperado. É útil manter esta interpretação em mente ao considerar suposições de confiança para os modelos de gerenciamento de identidade (JOSANG et al., 2005).

Conforme Bhargav-Spantzel et al. (2007), os principais elementos que participam do sistema de gerenciamento de identidades são:

- **Sujeito/Usuário (User):** entidade que possui pelo menos uma identidade digital e deseja realizar uma transação.
- **Identidade (Identity):** conjunto de atributos de um sujeito (e.g. nome, endereço, filiação, data de nascimento).
- **Identity Provider (IdP):** tipo especial de provedor de serviços que gerencia as informações de identidade e é responsável pela criação, manutenção e gerenciamento das informações de identidade, fornecendo serviços de autenticação do sujeito.
- **Service Provider (SP):** entidade que decide fornecer seus serviços com base nas informações fornecidas por outras partes, como um provedor de identidade e o próprio sujeito.

## A.2 EVOLUÇÃO DOS MODELOS DE GERENCIAMENTO DE IDENTIDADE

O gerenciamento de identidades digitais modificou-se constantemente, conforme a Internet e suas tecnologias foram avançando. No seu caminho evolutivo existem cinco estágios, ou modelos de desenvolvimento, conforme Figura 29.

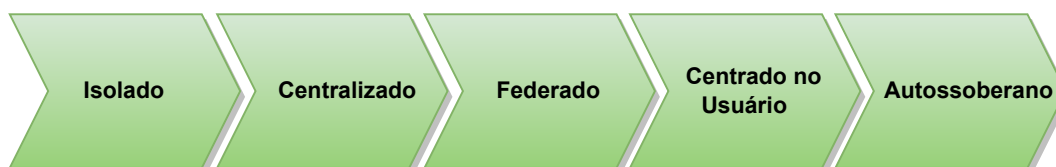


Figura 29 – Evolução dos Modelos de Gerenciamento de Identidade

### A.2.1 Modelo Isolado

Nesse modelo todo o controle da identidade é feito por uma única entidade que atua como *Identity Provider* e *Service Provider*, forçando o usuário a criar uma identidade para cada serviço isolado que ele deseja interagir (Figura 30) (JOSANG et al., 2005; JOSANG; ALZOMAI; SURIADI, 2007).

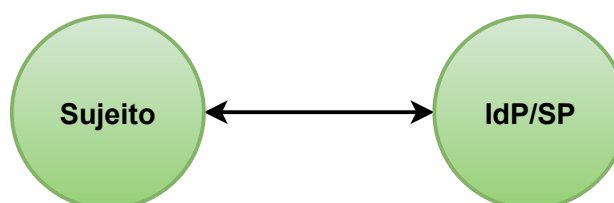


Figura 30 – Modelo de Gerenciamento de Identidade Isolado

O resultado deste modelo foi que os usuários têm que administrar identidades digitais espalhadas pelos diversos serviços online, rotineiramente esquecendo senhas não utilizadas de forma frequente, ou até mesmo abusando do uso de senhas de baixa entropia (JOSANG; ALZOMAI; SURIADI, 2007). Além disso, cada provedor de serviços online tem que arcar com os custos e dificuldades de implementação e manutenção de um sistema de gerenciamento de identidades, o que envolve a proteção contra possíveis ataques e vulnerabilidades (SCHARDONG; CUSTÓDIO, 2021).

O Modelo Isolado é amplamente utilizado nos atuais sistemas computacionais presentes na Internet (ALLEN, 2016), e a simplicidade de sua arquitetura torna relativamente fácil de entender e resolver os problemas de confiança envolvidos. A complexidade da confiança é bastante simplificada quando a mesma entidade atua como *Identity Provider* e *Service Provider* pois, nessas condições, o sujeito e o *Service Provider* só precisam confiar um no outro (JOSANG et al., 2005). O nível de confiança dos processos e mecanismos usados para registro de identidade e autenticação será definido pelo *Service Provider* de acordo com sua avaliação dos riscos e da sensibilidade

do serviço oferecido, *e.g.*, mecanismos mais robustos normalmente serão necessários para serviços bancários do que para acesso à uma biblioteca online.

### A.2.2 Modelo Centralizado

No Modelo Centralizado, há uma separação das funções do *Identity Provider* e do *Service Provider* que possibilita que cada sujeito possa utilizar a mesma identidade para acessar diferentes provedores de serviço (JOSANG et al., 2005), conforme Figura 31. O *Service Provider*, quando precisa autenticar um sujeito, envia as informações de identidade do mesmo para o *Identity Provider* concluir o processo (LÓPEZ, 2020).

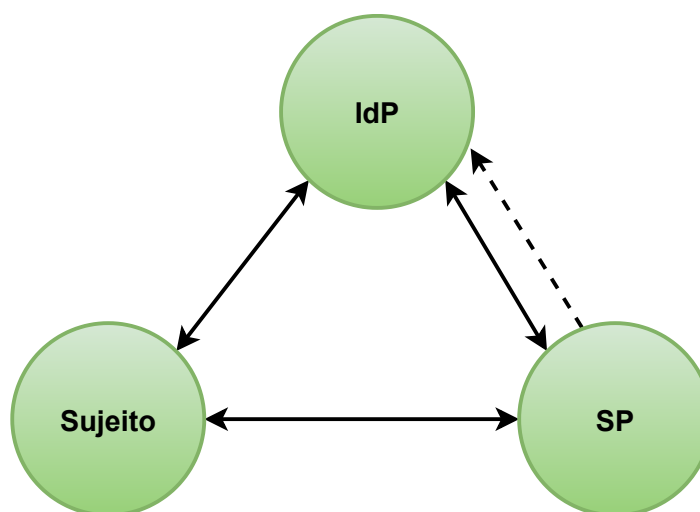


Figura 31 – Modelo de Gerenciamento de Identidade Centralizado

Esse modelo trouxe vantagens para o sujeito, pois reduz drasticamente a gestão problemática do usuário administrar várias identidades (JOSANG; ALZOMAI; SURIADI, 2007; SCHARDONG; CUSTÓDIO, 2021), porém, assim como no modelo isolado, os *Identity Providers* são obrigados a manter infra-estruturas robustas e assumem custos elevados para fornecer armazenamento seguro. Além de se tornarem ponto único de falha, como o número de *Identity Providers* é baixo comparado ao Modelo Isolado, há uma monopolização que impacta tanto em segurança quanto em confiabilidade (LÓPEZ, 2020) na medida que acaba criando silos de informações privadas valiosas (SCHARDONG; CUSTÓDIO, 2021).

### A.2.3 Modelo Federado

Os modelos de identidade federados são baseados em grupos de *Service Providers* que estabelecem um acordo mútuo de segurança e autenticação e estão ligados entre si para formar um domínio de confiança federado (JOSANG; ALZOMAI; SURIADI, 2007). Uma federação é um conjunto de acordos, padrões e tecnologias que

permitem a um grupo de *Service Providers* reconhecer identidades de outros *Service Providers*, dentro do domínio federado (JOSANG et al., 2005) (Figura 32).

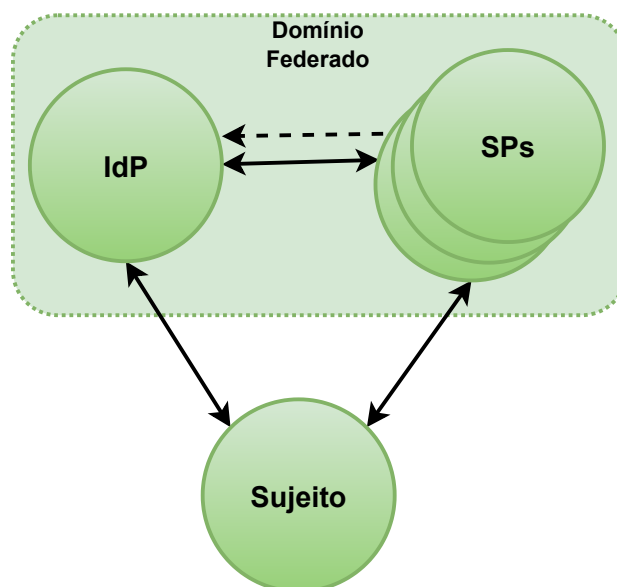


Figura 32 – Modelo de Gerenciamento de Identidade Federado

Em um domínio federado, cada *Service Provider* ainda fornece uma identidade separada para o mesmo usuário, mas este não precisa necessariamente usá-la. Na sua implementação mais comum, o acesso acontece por meio de um único *Service Provider*, permitindo que uma única identidade seja usada para acessar todos os demais *Service Providers* dentro do domínio federado (JOSANG et al., 2005).

Esse método de acesso é um caminho secundário que não requer as credenciais de autenticação do usuário. Este acesso indireto simplesmente requer a passagem de declarações de segurança, como por exemplo afirmações SAML (HIRSCH; PHILPOTT; MALER, 2004), entre *Service Providers*. A autenticação do usuário por outro *Service Provider* baseia-se nessas premissas. Dessa forma, problemas de segurança podem ocorrer se o *Service Provider* que realizou a autenticação inicial sofreu uma falha de autenticação ou enviou uma solicitação de acesso fraudulenta, *i.e.*, não em nome do usuário.

Convém ressaltar que as relações de confiança entre as partes podem ser complexas de estabelecer, *e.g.*, um banco que presta serviços à uma companhia aérea. Neste caso, os diferentes papéis desempenhados pelos *Service Providers* significa que eles estão expostos a diferentes riscos no caso de falha, *e.g.*, a falha de processamento financeiro das reservas online pode fazer com que a companhia aérea tenha uma perda financeira maior do que o banco, que apenas perderá algumas comissões de baixo valor. Neste caso, uma das partes tem exposição ao risco significativamente maior do que a outra, e portanto, os acordos comerciais e legais tornam-

se mais complexos.

Com base nesses fatores, embora o modelo federado tenha como objetivo simplificar a experiência do usuário evitando que estes tenham que lidar com diversas identidades, ele cria uma considerável complexidade de confiança para os *Service Providers* (JOSANG et al., 2005).

#### A.2.4 Modelo Centrado no Usuário

O Modelo Centrado no Usuário foi construído com base na ideia de que os usuários podem usar dispositivos pessoais para armazenar suas identidades, eliminando assim a necessidade de *Identity Providers* de terceiros e permanecendo com o controle de seus dados (Figura 33). Josang e Pope (2005) apresentaram este modelo em 2005, nomeando o hardware usado para armazenar os dados de *Personal Authentication Device* (PAD) (JOSANG; POPE, 2005).

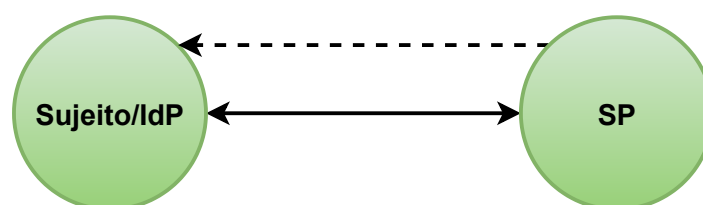


Figura 33 – Modelo de Gerenciamento de Identidade Centrado no Usuário

Deste modo, uma identidade centrada no usuário surgiu do desejo de que um usuário tenha mais controle sobre sua identidade e que a confiança fosse descentralizada, na medida em que as identidades ficariam em cada PAD (ALLEN, 2016). Porém se o usuário apenas armazena identidades para acessar *Service Providers* então este modelo, centrado no usuário, poderia ser entendido como um modelo centralizado, no qual o *Service Provider* permite autenticar com uma chave armazenada no PAD, em vez de um nome de usuário e senha (LÓPEZ, 2020), e, portanto, apresentando os mesmos problemas de controle, segurança e confiabilidade do modelo centralizado.

#### A.2.5 Modelo Autossoberano

No Modelo *Self-Sovereign Identity* (SSI), o indivíduo, a quem a identidade pertence por completo, controla e gerencia sua identidade (ALLEN, 2016). Ao contrário dos modelos isolados, centralizados, e federados, o modelo SSI não requer uma entidade para gerenciar a identidade das pessoas. A função do *Identity Provider* é limitada à ser um emissor de identidade (LÓPEZ, 2020) (Figura 34).

Segundo Christopher Allen (ALLEN, 2016), neste modelo a existência digital do indivíduo é independente de qualquer organização individual. Nos modelos anteriores não existe autonomia do usuário e este é o coração da identidade autossoberana.

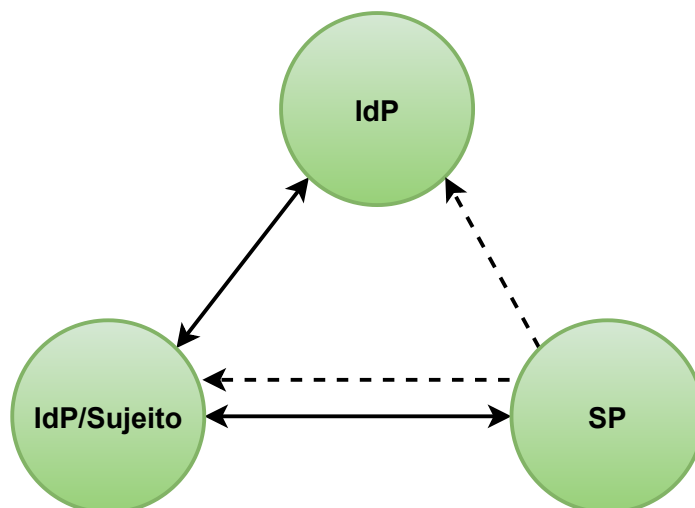


Figura 34 – Modelo de Gerenciamento de Identidade Autossobrerano

Em vez de apenas defender que os usuários estejam no centro do processo de identidade, a identidade autossobrerana exige que os usuários sejam os governantes de sua própria identidade.

Uma das primeiras referências à soberania de identidade ocorreu em fevereiro de 2012, quando Devon Loffreto escreveu sobre *“Sovereign Source Authority”* (LOFFRETO, 2012), declarando que os indivíduos “têm um direito estabelecido a uma identidade”, mas que o registro nacional destrói essa soberania (ALLEN, 2016). Desde então, a ideia de identidade autossobrerana proliferou.

Esse modelo de identidade traz consigo uma mudança fundamental na forma como os indivíduos interagem com seus dados pessoais. Ao capacitar os usuários a terem controle total sobre sua própria identidade digital, o SSI promove não apenas a segurança e privacidade dos dados, mas também a autonomia e a liberdade individual. Além disso, ao descentralizar o gerenciamento de identidade, o SSI reduz a dependência de entidades centralizadas, mitigando assim o risco de violações de dados em larga escala e fortalecendo a resiliência do ecossistema digital.

### A.3 COMPARAÇÃO ENTRE OS MODELOS DE GERENCIAMENTO DE IDENTIDADE

Os modelos apresentados diferem em diversos aspectos, seja na maneira como as identidades dos usuários são armazenadas e disponibilizadas, formas de autenticação, segurança ou usabilidade. Todavia, é essencial que um sistema de gerenciamento de identidades garanta uma melhor experiência de uso para os usuários sem que isso afete a segurança de suas informações pessoais.

Para fins de comparação, a Tabela 4 analisa os modelos de gerenciamento de identidade, considerando os elementos essenciais que Kim Cameron (CAMERON,

2005) julga necessários para que um sistema de identidades obtenha sucesso, apresentados na Seção 2.

Tabela 4 – Comparação entre os Modelos de Gerenciamento de Identidade

	<b>Isolado</b>	<b>Centralizado</b>	<b>Federado</b>	<b>Centrado no Usuário</b>	<b>Autossobrerano</b>
<b>Usuário pode gerar seus próprios identificadores</b>	N	N	N	N	S
<b>Usuário controla suas próprias credenciais</b>	N	N	N	S	S
<b>Usuário pode recuperar suas credenciais com facilidade</b>	S	S	S	N	S
<b>Disponibilidade de transportar credenciais de um provedor para outro (Portabilidade)</b>	N	N	N	N	S
<b><i>Identity Provider</i> não mantêm bases centralizadas com dados dos usuários</b>	N	N	N	N	S
<b><i>Identity Provider</i> não têm informações sobre o acesso ou interações dos usuários com serviços</b>	N	S	S	S	S
<b>Violações de dados menos prováveis</b>	N	N	N	N	S
<b>Experiência do usuário consistente em vários contextos e tecnologias</b>	N	N	N	N	S
<b>Ausência de ponto único de falha</b>	N	N	S	N	S

Fonte: Autor

## ANEXO B – FRAMEWORKS SSI

Para qualquer entidade do ecossistema SSI, a segurança e a privacidade dos seus dados pessoais são de extrema importância. Nesse sentido, a ideia principal do modelo SSI, de descentralizar o armazenamento das identidades na forma de credenciais verificáveis, permite que as entidades controlem o uso de seus próprios dados em um ecossistema descentralizado.

Existem princípios definidos para uma solução SSI, como os descritos por Christopher Allen (ALLEN, 2016), e que servem como um guia para as soluções SSI propostas. Exemplificadamente, o controle e a segurança são destaques como princípios propostos, assim como a portabilidade e interoperabilidade também são propriedades desejadas para se ter uma adoção mais ampla. À vista disso, o Wide Web Consortium (W3C) tem se esforçado para criar padrões para estabelecer a interoperabilidade e portabilidade de identidades e credenciais, bem como facilitar a sua troca e gerenciamento.

No Capítulo 2, foi visto que as arquiteturas de soluções SSI requerem o uso de *Distributed Ledger Technology* (DLT) como um bloco de construção essencial, e a blockchain é a plataforma DLT mais comum para o desenvolvimento dessas soluções pois, na medida em que os dados armazenados são protegidos usando ferramentas criptográficas, uma solução SSI baseada em blockchain promove a segurança e privacidade entre os participantes da rede.

Para facilitar a criação do ecossistema SSI, *frameworks* são criados para suportar esse desenvolvimento. Dessa forma, nesse capítulo são apresentados os *frameworks* para desenvolvimento de soluções de SSI, baseados em blockchain, mais comumente usados, bem como uma análise comparativa entre eles.

### B.1 BLOCKCHAIN

A rigor, pode-se dizer que a *Distributed Ledger Technology* (DLT) é uma combinação de várias tecnologias que suportam um sistema distribuído de base de dados, mantido e gerido de forma compartilhada e descentralizada por meio de uma rede *peer-to-peer* (P2P), na qual todos os participantes são responsáveis por armazenar e manter a base de dados de forma confiável e segura (MARINO et al., 2019).

Na visão da *International Telecommunication Union* (ITU), as DLTs, cuja implementação mais proeminente é a blockchain, permitem que nós, em uma rede distribuída, cheguem a um acordo e registrem informações sem a necessidade de uma

autoridade central. Blockchain é um tipo de DLT composto de dados gravados digitalmente, organizados como uma cadeia de blocos em crescimento sucessivo, com cada bloco criptograficamente vinculado e reforçado contra adulteração e revisão (ITU, 2019).

A tecnologia blockchain foi construída tendo em mente quatro principais características arquiteturais: (i) segurança das operações, (ii) descentralização de armazenamento e computação; (iii) integridade de dados e (iv) imutabilidade de transações. Desta forma, blockchain é um *'ledger of facts'* replicado em computadores que participam de uma rede *peer-to-peer*, no qual (YAGA et al., 2019):

- O *ledger* é um livro de registros digital, no qual, uma vez validado um registro, este nunca mais poderá ser apagado.
- Um fato (*fact*) pode significar várias coisas, desde uma transação monetária até o conteúdo de determinado documento.
- Os membros participantes da rede podem, ou não, ser anônimos e são chamados nós (*peers*).
- Toda transação dentro do *ledger* é protegida por tecnologias criptográficas de assinatura digital, inclusive para identificar os nós emissores e receptores das transações.
- Quando um nó deseja adicionar ao *ledger* um fato novo, é necessário um consenso entre todos ou alguns nós previamente determinados da rede, para decidir se um fato pode ser registrado no ledger.
- Havendo consenso, o fato será escrito e nunca mais poderá ser apagado.

Segundo Buterin (BUTERIN, 2015), a blockchain pode ser classificada em três principais modelos, diferenciados pelo seu acesso, que são blockchain pública, consorciada e privada. A blockchain pública é um modelo com uma plataforma de contabilidade totalmente descentralizada e aberta para que qualquer usuário possa publicar blocos, ler estes blocos/transações e validar transações. A blockchain consorciada é um modelo composto por duas ou mais instituições pré-definidas, nas quais os usuários participantes necessitam de autorização para publicarem novos blocos, sendo estas redes parcialmente descentralizadas. Por fim, a blockchain privada é um modelo semelhante ao modelo consorciado, com a diferença de que nesta rede apenas uma instituição é administradora. A redes privadas possuem a instituição mantenedora como pré-definida e os usuários participantes necessitam de autorização para a publicação de novos blocos.

## B.2 BLOCKCHAIN E SSI

De fato, a tecnologia blockchain melhora o gerenciamento de identidade de várias maneiras. As assinaturas digitais, um dos principais componentes da tecnologia blockchain, fornecem autenticidade da prova e atestado de identidade enquanto a rede *peer-to-peer* elimina a necessidade de um repositório central da identidade dos usuários, tornando as soluções resistentes a adulterações e melhorando a segurança e a privacidade (ZAEEM et al., 2021)

Nesse sentido, especificamente para as soluções SSI, os benefícios do uso de blockchain foram resumidos na Tabela 5.

Tabela 5 – Benefícios da blockchain em SSI

<b>Benefício</b>	<b>Descrição</b>
Transações confiáveis, rápidas e sem intermediários	Reduz ou mesmo elimina o risco da desconfiança entre as partes e custos de transação.
Usuários com poderes	Usuário controla todas as suas transações e informações
Dados de alta qualidade	Os dados da blockchain intrinsecamente são completos, consistente, precisos e amplamente disponíveis no momento que forem necessários.
Duráveis, confiáveis e amplamente disponíveis	Ausência de ponto único de falha
Processos íntegros	Confiança que tudo será executado conforme as regras pré-definidas sem intermediários.
Transparência e imutabilidade	Todas as transações podem estar disponíveis publicamente e não podem ser alteradas ou ainda apagadas dos registros.
Simplificação do ecossistema	Um único livro de registro é criado, reduzindo a desordem e complicações.

Fonte: (NAKAMURA et al., 2019)

Dessa forma, tendo que um dos problemas associado às identidades são os aspectos relacionados a segurança e privacidade, e dado que a blockchain assegura a transparência e a integridade das transações que ela contém, diversas plataformas blockchain foram exploradas para desenvolver *frameworks* para soluções SSI baseados em blockchain (MARINO et al., 2019). Em seguida, são exploradas as funcionalidades dos *frameworks* mais comumente usados.

## B.3 SHOCARD

O ShoCard (SHOCARD, 2019) é um sistema de gerenciamento de identidade que utiliza uma blockchain pública, e funciona buscando mapear credenciais tradicionais, normalmente físicas, digitalizando-as e publicando um *hash* em um livro razão público distribuído. Dessa forma, os usuários escaneiam suas credenciais, *e.g.* o passaporte, e os atributos são armazenados nos próprios dispositivos móveis dos

usuários. Um *hash* assinado desses dados, chamado ShoCardID, é armazenado em transações da blockchain Bitcoin.

Em uma segunda etapa, esses dados são certificados por um provedor de identidade (SOLTANI; NGUYEN; AN, 2018), conferindo ao ShoCard um status parcialmente centralizado na medida em que cria instabilidade na existência do ShoCardID pois, se os provedores de identidade pararem de funcionar, os detentores de identidade não poderão usar suas credenciais digitais (SHUAIB et al., 2022).

Além disso, como o ShoCard utiliza em suas transações a blockchain Bitcoin, que demora em média 10 minutos para minerar as transações e realiza a espera por seis blocos adicionais para liquidação de uma transação, implica dizer que esta é uma restrição que limita o uso do ShoCard à cenários que exigem apenas identidades predefinidas (os atributos são conhecidos com antecedência), uma vez que não é possível criar identidades em tempo real (SHUAIB et al., 2022).

#### B.4 CIVIC

O Civic é um sistema de identidade descentralizada, baseado na blockchain Ethereum, que utiliza contratos inteligentes para as validações das identidades. A identidade Civic permite que os usuários possam monitorar seus dados e compartilhar apenas as informações que estão dispostos. Um aplicativo Civic é usado para armazenar informações de identidade de forma criptografada, em um dispositivo móvel. O valor do *hash* das informações de identidade é armazenado na blockchain (TECHNOLOGIES, 2017).

O Civic permite que os proprietários de identidade divulguem dados seletivamente e que provedores de identidade, conhecidos como validadores, participem e assinem transações em nós públicos da blockchain. Isto propicia um sistema aberto interativo para o validador, porém não totalmente descentralizado, na medida em que os usuários dependem das autoridades de autenticação para estabelecer uma identidade digital protegida (SHUAIB et al., 2022).

#### B.5 SOVRIN

Sovrin é uma rede de identidade descentralizada de código aberto construída sobre a tecnologia DLT. É considerada uma rede pública/permissionada, constituída apenas de instituições confiáveis, - que podem ser bancos, universidades, governos, instituições de pesquisa - sendo estas os nós, que participam do consenso e executam a gravação na *ledger*. Os nós observadores só possuem atributo de leitura da *ledger* e atuam como intermediários entre o usuário final e a rede (TOBIN; REED,

2017). A Fundação Sovrin, sem fins lucrativos, assegura a governança adequada dos administradores e o respeito ao acordo legal denominado '*Sovrin Trust Framework*'.

A Sovrin permite que um usuário gere tantos identificadores quantos forem necessários para manter a separação contextual de identidades para fins de privacidade. Cada identificador é único e controlado por um par de chaves assimétricas distintas (REED; LAW; HARDMAN, 2019). Os identificadores da Sovrin são gerenciados pelo usuário ou por um serviço intermediário designado (agente), e seguem a especificação de *Decentralized Identifiers* (DIDs), padrão W3C.

O elemento chave da arquitetura da Sovrin é a sua própria blockchain chamada *Sovrin Ledger*. Essa blockchain contém transações associadas a um identificador específico, que são gravadas, distribuídas e replicadas entre os nós, que executam uma versão aprimorada do protocolo redundante de tolerância a falhas bizantina (AUBLIN et al., 2015), chamado Plenum, para consenso (FERDOUS; CHOWDHURY; ALASSAFI, 2019).

Em 2017 a Sovrin Foundation transferiu o código open-source para a Linux Foundation a qual deu origem ao Hyperledger Indy. Atualmente, a Sovrin usa o Hyperledger Indy como base de código para a sua rede.

## B.6 UPORT

O uPort é um sistema de identidade descentralizada de código aberto, construído sobre a plataforma blockchain Ethereum. Consiste em um aplicativo móvel e vários contratos inteligentes Ethereum (LUNDKVIST et al., 2019).

Um usuário utiliza um aplicativo móvel para criar, atualizar e compartilhar informações de identidade com outros usuários. No *backend*, esses dados são controlados por contratos inteligentes. A maior parte dos dados de identidade são armazenados em um *InterPlanetary File System* (IPFS), que é um sistema de arquivos distribuído em que um arquivo pode ser recuperado por seu *hash* criptográfico, enquanto o aplicativo móvel é usado para armazenar a chave privada correspondente de uma identidade uPort. O registro público é usado para criar uma correlação entre uma identidade uPort e seus dados IPFS correspondentes (NAIK; JENKINS, 2020).

## B.7 HYPERLEDGER INDY, ARIES E URSA

O *framework* Hyperledger Indy, em conjunto com o Hyperledger Aries e Hyperledger Ursa são oferecidos pelo Hyperledger Greenhouse, um consórcio de código aberto para o desenvolvimento de tecnologias blockchain, hospedado pela Linux Foundation. O Hyperledger Indy é uma pilha de desenvolvimento que fornece ferramentas,

bibliotecas e componentes para criação de sistemas que consigam prover soluções para identidades digitais, utilizando arquiteturas como a blockchain ou outra tecnologia de livro razão distribuídos (INDY, 2022).

As principais tecnologias que sustentam o Hyperledger Indy são (SOLTANI; NGUYEN; AN, 2018):

- Livro razão distribuído para identidade descentralizada.
- *Design* resistente à correlação de dados.
- Uso de identificadores descentralizados (DIDs).
- Credenciais verificáveis em um formato interoperável.
- Suporte à *Zero-Knowledge Proof*.

O registro distribuído do HyperLedger Indy é do tipo público permissionado. Permissionado na validação, pois é necessário uma permissão (papel específico na rede chamado de nó validador) para participar da validação e escrita das transações, e público pois o acesso à leitura é aberto (BHATTACHARYA; ZAVARSKY; BUTAKOV, 2020). Os nós validadores executam o algoritmo de consenso Plenum, que é uma implementação aprimorada do protocolo de consenso de tolerância a falhas bizantinas (SOLTANI; NGUYEN; AN, 2018). Nenhum dado privado é escrito na blockchain. São escritos apenas DIDs públicos, chaves públicas, esquemas de credenciais e informações sobre revogações, garantindo assim a privacidade dos dados. As requisições de escrita necessitam de autenticação e devem ser assinadas digitalmente, enquanto as requisições de leitura não necessitam nenhum tipo de autenticação (acesso público).

O Indy apoia-se no Hyperledger Ursa (URSA, 2022) que é a biblioteca que provê os métodos criptográficos e no Hyperledger Aries, que provê a infraestrutura para criar, transmitir e armazenar credenciais verificáveis. O Aries possui uma camada de interface para criar, assinar e ler transações na blockchain, fornecendo suporte para trocas e emissão de credenciais verificáveis, incluindo credenciais que utilizam a *Zero-Knowledge Proof*, encontradas na biblioteca Ursa (ARIES, 2022).

O Aries possui como suas principais características:

- Uma interface para criação, assinatura e leitura de transações em uma blockchain.
- Um sistema de armazenamento seguro para guardar as credenciais verificáveis, as chaves criptográficas e qualquer outra informação utilizada para a gestão das credenciais verificáveis.

- Um protocolo de comunicação *peer-to-peer* baseado nos DIDs.
- Suporte para a utilização de primitivas ZKP disponíveis na biblioteca Ursa para realizar a emissão ou prova de credenciais verificáveis.
- Diversos protocolos que permitem a implementação de agentes Aries interoperáveis.
- Um conjunto de diversas implementações pré desenvolvidas já disponíveis para implementações como carteiras digitais, por exemplo.
- Um agente de teste que permite o teste de interoperabilidade entre os agentes e seus *frameworks*.

## B.8 COMPARAÇÃO ENTRE OS PRINCIPAIS *FRAMEWORKS* SSI

As soluções apresentadas diferem em diversos aspectos, seja no modelo de atuação, na arquitetura apresentada, nas tecnologias blockchain utilizadas e nos desafios encontrados. Os critérios de avaliação estabelecidos para fins de comparação, são baseados nos princípios que definem um sistema SSI, descritos por Christopher Allen e apresentados na Seção 2. Dessa forma, com base nos *frameworks* SSI detalhados anteriormente, a Tabela 6 fornece uma análise comparativa dessas soluções.

Tabela 6 – Comparação entre os *Frameworks* SSI

	Sovrin	ShoCard	uPort	Civic	Indy
<b>Existência</b>	S	S	S	S	S
<b>Controle</b>	S	S	S	S	S
<b>Acesso</b>	S	S	S	S	S
<b>Transparência</b>	S	S	S	S	S
<b>Persistência</b>	S	N	S	N	S
<b>Portabilidade</b>	S	N	S	N	S
<b>Interoperabilidade</b>	S	S	S	S	S
<b>Consentimento</b>	S	S	S	S	S
<b>Minimização</b>	-	-	-	-	S
<b>Proteção</b>	S	N	S	N	S

Fonte: Autor

Como é evidente na Tabela 6, a maioria dos *frameworks* satisfazem a maior parte dos princípios que definem um sistema SSI, à exceção do Hyperledger Indy, que cumpre todos. Nessa análise pode-se observar que o ShoCard não está cumprindo o princípio de proteção, portabilidade e persistência devido à sua dependência parcial de um IdP centralizado para validação de identidades; o Civic, do mesmo modo, não está em conformidade com o princípio de proteção, portabilidade e persistência devido

à sua dependência de terceiros; o uPort, apesar de cumprir com os princípios SSI, permite criar apenas uma identidade por indivíduo, portanto, um usuário não pode criar diversas identidades conforme o contexto, dessa forma, conclui-se que não suporta autonomia total.

Mesmo que o Sovrin afirme oferecer suporte à portabilidade, propõe um padrão para representar uma identidade, portanto, se sua proposta não for padronizada em todos os sistemas perderá seu recurso de portabilidade. No entanto, entre essas soluções analisadas, o Hyperledger Indy é o único que atende todos os princípios do SSI. Um fator não analisado é o custo, pois todas as soluções incorrem em custos para criar transações ou armazenar dados em suas respectivas plataformas blockchain. Dependendo do custo incorrido, pode criar uma barreira adicional para qualquer adoção em larga escala.

## ANEXO C – HYPERLEDGER INDY

Dado que a solução desenvolvida integra componentes concebidos pela comunidade Hyperledger, tais como os projetos Indy Plenum, Indy Node, Indy SDK e a biblioteca criptográfica Ursa, este Anexo apresenta uma breve explicação desses projetos e sua relevância dentro do contexto da solução. O Hyperledger Indy é um projeto *open source* desenvolvido pela comunidade Hyperledger e apoiado pela Linux Foundation (FOUNDATION, 2023), que implementa os padrões de identidade descentralizada definidos pelo W3C (W3C, 2022).

Este projeto tem como base uma blockchain pública e permissionada, construída com o propósito de ser usada para gestão de identidades descentralizadas, na qual qualquer utilizador pode efetuar operações de leitura, mas apenas nós com permissão podem efetuar operações de escrita. Através das suas várias características e funcionalidades, o Hyperledger Indy (INDY, 2022) é um projeto que:

- Apresenta um registo distribuído construído especificamente para identidade descentralizada.
- Por *design*, é resistente à correlação.
- Suporta a utilização de DIDs.
- Disponibiliza o uso de divulgação seletiva e ZKP.
- Fornece às entidades o controle sobre as suas credenciais.
- Dá suporte aos dez princípios do SSI abordados no Capítulo 2.

Dada a sua dimensão, o projeto Hyperledger Indy está dividido em várias componentes, cujos principais são o Indy Plenum (PLENUM, 2023), o Indy Node (NODE, 2023), o Indy SDK (SDK, 2023), o Aries Agent (ARIES, 2022) e a biblioteca Ursa (URSA, 2022). As subseções seguintes visam explicar de forma resumida em que consiste cada um dos projetos indicados.

### C.1 INDY PLENUM

O Indy Plenum (PLENUM, 2023) é responsável por gerir o *ledger*, definindo o protocolo de consenso e as várias operações criptográficas da blockchain. O Indy possui uma blockchain pública quanto ao acesso (no qual qualquer Utilizador pode ler

o conteúdo da mesma), e permissionada quanto à validação (quando apenas Utilizadores com permissões podem submeter transações).

O algoritmo de consenso utilizado pelo Indy é o *Plenum Byzantine Fault Tolerant Protocol* (PRBFT) (PLENUM, 2023), uma implementação do algoritmo de tolerância redundante a falhas bizantinas (RBFT) (AUBLIN; MOKHTAR; QUÉMA, 2013) com algumas alterações. O RBFT por sua vez é baseado no algoritmo *Byzantine Fault Tolerance* (BFT) que procura resolver o problema dos generais bizantinos, e baseia-se na necessidade de assegurar que os generais estabelecem consenso num plano de batalha, comunicando entre si através de mensageiros.

## C.2 INDY NODE

O Indy Node (NODE, 2023) é responsável por realizar a gestão de nós, adição, alteração e remoção de permissões, e ainda oferecer suporte à transações específicas de um sistema SSI, sendo responsável por processar cada transação de acordo com o seu tipo. Sendo o Indy uma blockchain permissionada, apresenta um conjunto de papéis com permissões diferentes para lidar com os vários tipos de Utilizadores da rede: *trustee*, *steward*, *endorser*, *network monitor* e *identity owner*. Adicionalmente, por ser uma blockchain baseada em permissões, deve também conter um conjunto de transações iniciais que definem as várias entidades com as permissões mais elevadas, *i.e.*, os *trustees* e os *stewards*, que são responsáveis por atribuir permissões aos restantes Utilizadores da rede.

### *Operações de escrita e leitura*

Dado que para uma blockchain todas as transações são apenas conjuntos de dados, o Indy Node diferencia os vários tipos de transações através do atributo *type*. Na Figura 35 é possível observar que o valor do campo *type* identifica qual a operação que deverá ser executada. Esta operação pode ser de escrita ou de leitura dependendo do código.

```
{
  "operation": {
    "type": <request type>, // tipo de pedido
    <request-specific fields> // campos específicos do pedido
  },
  "identifier": <author DID>,
  "endorser": <endorser DID>,
  "reqId": <req_id unique integer>,
  "protocolVersion": 2,
  "signature": <signature_value> // valor da assinatura
}
```

Figura 35 – Estrutura de um pedido à blockchain

As Figuras 36(a) e 36(b) indicam todas as operações disponibilizadas pelo Indy Node e quais os códigos associados as mesmas. Adicionalmente, com o objetivo

de aumentar a flexibilidade das operações, podem ser adicionados atributos específicos do pedido ao atributo *operation*. O documento Hyperledger Indy Node Documentation (NODE, 2023) detalha cada uma destas operações bem como os atributos adicionais que cada uma delas pode receber. No final da estrutura JSON é possível observar ainda o atributo *signature*. Este atributo é utilizado para autenticar os autores das transações enviadas para a blockchain, e é obrigatório em todas as operações de escrita.

<pre>NODE = '0' NYM = '1' TXN_AUTHOR_AGREEMENT = '4' TXN_AUTHOR_AGREEMENT_AML = '5' ATTRIB = '100' SCHEMA = '101' CLAIM_DEF = '102' POOL_UPGRADE = '109' NODE_UPGRADE = '110' POOL_CONFIG = '111' REVOC_REG_DEF = '113' REVOC_REF_ENTRY = '114' AUTH_RULE = '120' AUTH_RULES = '122'</pre>	<pre>GET_TXN = '3' GET_TXN_AUTHOR_AGREEMENT = '6' GET_TXN_AUTHOR_AGREEMENT_AML = '7' GET_ATTRIB = '104' GET_NYM = '105' GET_SCHEMA = '107' GET_CLAIM_DEF = '108' GET_REVOC_REG_DEF = '115' GET_REVOC_REG = '116' GET_REVOC_REF_DELTA = '117' GET_AUTH_RULE = '121'</pre>
(a) Tipos de operações de escrita	(b) Tipos de operações de leitura

Figura 36 – Tipos de operações de escrita e de leitura

### *Sistema de permissões da blockchain*

A execução de operações de leitura não requer quaisquer permissões, de modo que todos os Utilizadores do sistema as podem efetuar. Relativamente às operações de escrita, algumas operações só estão disponíveis para Utilizadores com um determinado tipo de papel (*e.g.* apenas *trustees* podem adicionar outros *trustees*) enquanto que outras só estão disponíveis para Utilizadores específicos (*e.g.* alterar um atributo dentro de um documento de um DID apenas pode ser efetuado pelo dono desse DID).

Antes de analisar o sistema de permissões das operações de leitura e escrita, é necessário caracterizar os vários tipos de Utilizadores existentes: *trustee*, *steward*, *endorser*, *network monitor* e *identity owner*.

- *Trustee* representam as entidades mais confiáveis e com mais permissões do sistema e é responsável pela gestão do *pool* de nós e pelo estabelecimento das regras de autenticação.
- *Steward* é o papel desempenhado por entidades públicas que estão dispostas a contribuir com nós para a execução do protocolo de consenso da blockchain.
- *Endorser* é o papel atribuído às entidades que estão dispostas a assumir a responsabilidade legal e o esforço necessário para ajudar os autores das transações.

ções a escreverem itens no *ledger*. Estas entidades também podem escrever no *ledger* transações da sua autoria, sendo esta a razão de alguns deles quererem ser *endorsers*. Deste modo, a maior parte dos Emissores acaba por pertencer a este grupo.

- *Network Monitor* corresponde ao papel desempenhado por entidades cuja função é garantir que os nós operem de forma eficiente.
- *Identity Owner* corresponde a todas as entidades que possuem identidade, geralmente designados por Titulares.

Como o Indy Node disponibiliza várias operações de leitura e escrita, para fins de simplificação, serão detalhadas apenas as mais comuns: NODE, NYM, ATTRIB e SCHEMA. As operações do tipo NYM permitem registrar, promover ou rebaixar Utilizadores. Uma transação NYM permite associar um DID à um dos cinco papéis indicados anteriormente, sendo esta transação necessária para que o dono desse DID possa efetuar operações de escrita na blockchain.

Utilizadores que não estão registrados na blockchain com algum dos papéis indicados apenas podem efetuar operações de leitura. Quanto ao registro e promoção de Utilizadores, um *trustee* pode atribuir qualquer um dos cinco papéis apresentados a qualquer Utilizador e um *steward* apenas pode adicionar *endorsers*, *monitors* e *identity owners* e promover Utilizadores já registados até ao nível de *endorser*, ou seja, não pode adicionar ou promover Utilizadores para o nível *steward* ou *trustee*. Os tipos restantes de Utilizadores não possuem permissões para alterar o papel de outros Utilizadores. Por sua vez, as operações do tipo NODE permitem efetuar uma gestão granular dos vários nós, sendo possível adicionar nós no estado ativo ou inativo, promover (ativar) e rebaixar (desativar) nós e alterar atributos desses nós, tais como o endereço de IP e a porta.

As operações do tipo ATTRIB permitem adicionar e editar atributos associados a um DID registrado na blockchain. O sistema permite que cada Utilizador possa adicionar os atributos que desejar, contudo a maioria dos Utilizadores de um sistema SSI interage com esse sistema através de agentes de Utilizadores. É portanto responsabilidade destes agentes disponibilizarem mecanismos de adição e edição de atributos.

Na maioria dos casos de uso, o único atributo que precisa de ser armazenado na blockchain associado ao DID, é o seu respectivo documento. Por este motivo o agente de Utilizador apenas disponibiliza operações do tipo ATTRIB relacionadas ao atributo referente ao documento do DID. Apenas o dono de um DID presente na blockchain pode adicionar, alterar ou remover atributos associados a esse mesmo DID.

Por fim as operações do tipo SCHEMA permitem criar esquemas de credenciais verificáveis. Os quatro tipos de operações apresentados mostram que o sistema de permissões pode ser tão flexível quanto necessário, permitindo fornecer permissões de acordo com o papel dos Utilizadores ou com os seus DIDs específicos.

### C.3 INDY SDK

O Indy SDK consiste numa biblioteca *c-callable* e num conjunto de *wrappers* em várias linguagens para essa biblioteca. A biblioteca *c-callable* é escrita em C, e permite construir APIs para diversas linguagens diretamente sobre ela, o que elimina a necessidade de criar implementações específicas para cada uma dessas linguagens. Atualmente esta biblioteca apresenta *wrappers* para Java, Python, iOS, NodeJS, .Net e Rust.

A biblioteca Indy SDK contém várias operações relacionadas à criação de esquemas e credenciais, gestão de DIDs, entre outros, de acordo com os padrões propostos pelo W3C. Adicionalmente, implementa ainda uma carteira digital criptograficamente protegida, baseada em SQLite, que é armazenada do lado do utilizador (*i.e.* computador pessoal ou *smartphone*) e disponibiliza mecanismos que permitem substituir o núcleo desta carteira digital por uma implementação externa.

### C.4 ARIES AGENT

O Aries Agent representa o software responsável por interagir com o ecossistema em nome do utilizador através de comunicações ponto-a-ponto e com o auxílio da blockchain. O software deve ainda ser responsável por fornecer uma carteira digital segura ao utilizador e gerí-la de acordo com a vontade do mesmo, criando, armazenando e transmitindo credenciais verificáveis. Um agente SSI necessita realizar operações tais como criar esquemas, credenciais ou provas, armazenar ou consultar registros na carteira, entre outras. Estas operações são disponibilizadas pela biblioteca Indy SDK, razão pela qual é comum que um Aries Agent inclua a biblioteca Indy SDK para realizar tais operações.

### C.5 URSA

Por fim, a biblioteca Ursa contém várias operações criptográficas, entre as quais se destacam o esquemas de assinaturas Boneh–Lynn–Shacham (BLS), utilizadas na blockchain para garantir que todos os nós consentem com o estado atual do registro; o esquemas de assinaturas Camenisch-Lysyanskaya (CL), um formato de assinatura de provas de conhecimento zero utilizado pelo emissor para assinar os atributos presentes na credencial do titular; e ainda a técnica de criptografia simétrica

Chacha20-Poly1305, utilizada para cifrar os dados armazenados na carteira digital. Além destas técnicas, o projeto Ursa apresenta implementações de ECDSA, EdDSA, ECDH, AES-CBC, entre várias outras técnicas criptográficas que podem ser utilizadas fora do contexto de identidades digitais, razão pela qual esta biblioteca se individualizou num projeto isolado.

## ANEXO D – CASO DE USO

No Capítulo 5, Seção 5.2 foram descritos os fluxos de trabalho que envolvem as entidades da cadeia algodoeira, aos quais é possível aplicar a solução desenvolvida. Neste anexo, demonstra-se uma aplicação prática do COTTONTRUST envolvendo transações do tipo QUERY\_SEAL (Figura 37), que se refere à consulta do selo de certificação de um Fardinho de Algodão. Essa consulta é realizada por meio da verificação da credencial verificável correspondente ao selo de certificação, possibilitando confirmar a autenticidade do mesmo.

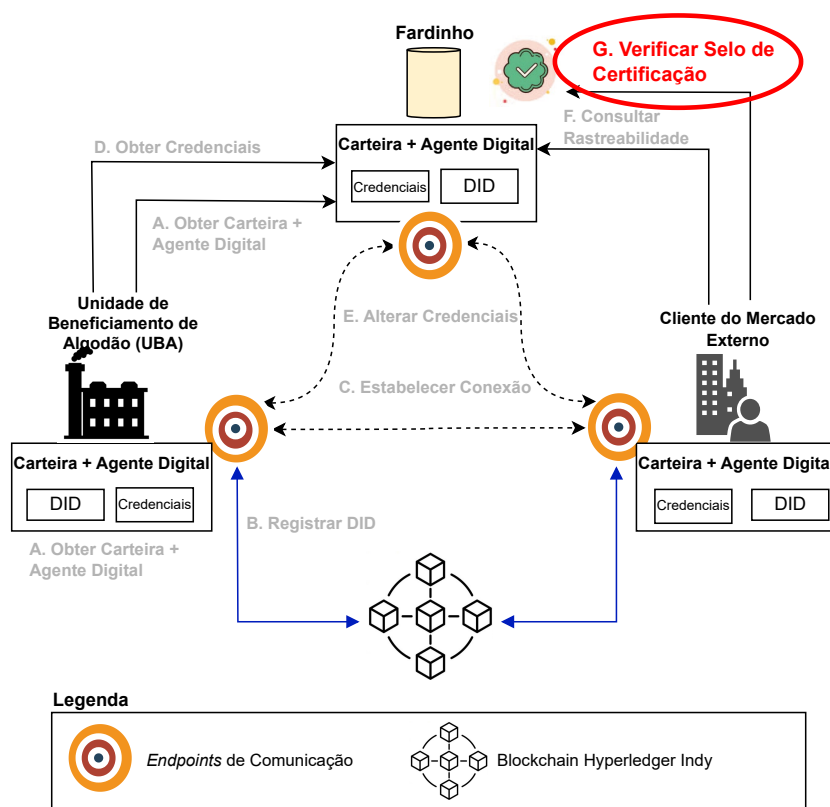


Figura 37 – Visão geral do funcionamento do COTTONTRUST destacando o fluxo de trabalho relacionado ao caso de uso

No cenário que envolve a verificação da legitimidade dos selos de certificação atribuídos a cada Fardinho de Algodão, o Comprador do Mercado Internacional manifesta o interesse em confirmar se um respectivo selo, emitido por determinado órgão de certificação, é autêntico. Diante desse desafio, após estabelecer uma conexão direta com o Fardinho, o Comprador solicita à carteira digital do Fardinho uma comprovação da autenticidade do selo em questão. O Fardinho possui uma credencial verificável que corresponde ao selo de certificação, e, nesse procedimento, é capaz de gerar apresentação verificável, *i.e.*, uma evidência concreta da autenticidade do

selo, e apresentá-la ao Comprador. Este, munido das informações contidas na referida apresentação verificável, consegue efetuar uma verificação precisa e imediata, assegurando-se da autenticidade do selo de certificação. O caso de uso exemplifica o cenário descrito, simulando uma carteira digital criada utilizando o framework React.JS (REACT.JS, 2023) (biblioteca front-end JavaScript de código aberto com foco em criar interfaces de usuário em páginas *web*).

Esse caso de uso é detalhado nas Seções D.1 e D.2, que apresentam o registro das entidades envolvidas; na sequência as Seções D.3, D.4 e D.5 descrevem os processos que envolvem a emissão das credenciais verificáveis relativas aos selos de certificação; e, por fim, a Seção D.6 exemplifica o processo de confirmação da autenticidade dos selos.

## D.1 CRIAÇÃO DE ENTIDADES

Esse caso de uso envolve três entidades: (i) **Emissor:** Órgão Certificador (OCE); (ii) **Titular:** Fardinho de Algodão (FAD); (iii) **Verificador:** Comprador do Mercado Internacional (CMI). Cada uma das entidades indicadas possui uma carteira digital e um agente digital, que lhe permite interagir com outras entidades. A carteira digital do OCE e CMI estão em seus dispositivos físicos pessoais e do FAD está na nuvem.

## D.2 CRIAÇÃO DE DIDs

Tanto o OCE (Emissor) como o CMI (Verificador) devem possuir DIDs públicos de modo a associarem a sua identidade digital à respectiva entidade física. Adicionalmente, o OCE precisa ser capaz de publicar esquemas e definições de credenciais na blockchain. Para tal, precisa de um DID público que lhe forneça as permissões necessárias. As permissões de autorização para publicação de transações na blockchain estão descritas no Anexo C, Seção C.2. As entidades poderão gerir os seus DIDs utilizando uma página de gestão de DIDs, apresentada na Figura 38.

No COTTONTRUST, o registro de DIDs públicos requer que uma entidade com permissões adequadas submeta transações de registro desses DIDs à blockchain. Tendo isso por base, tanto o OCE como o CMI necessitam registrar DIDs públicos na blockchain, recorrendo para tal, à uma entidade de maior autoridade (*e.g.* o estado brasileiro), que desempenhe o papel de *trustee*, *i.e.*, o papel com mais permissões dentro da blockchain. Por questões de simplicidade, esta entidade de maior autoridade não é considerada neste caso de uso, sendo utilizadas *seeds* que permitem importar DIDs já registrados na blockchain para a carteira digital, tal como mostra a Figura 39.

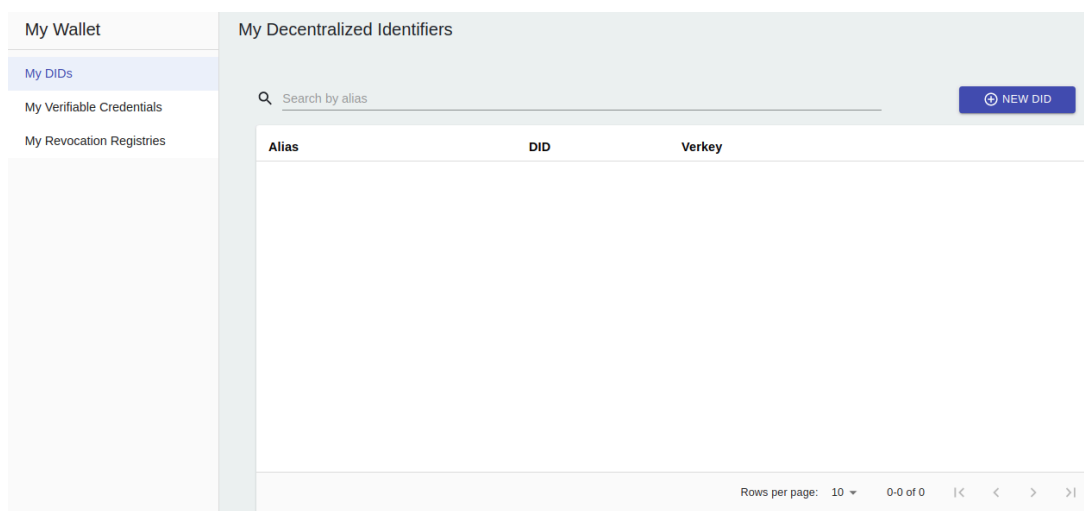


Figura 38 – Página de gestão de DIDs

Create a new DID

Alias \*

Seed

CANCEL CREATE

(a) DID público do OCE (steward)

Create a new DID

Alias \*

Seed

CANCEL CREATE

(b) DID público do CMI (steward)

Figura 39 – Criação dos DIDs públicos utilizando *seeds*

### D.3 CRIAÇÃO DE ESQUEMAS E DEFINIÇÕES DE CREDENCIAIS

Para iniciar o processo de emissão de credenciais correspondentes aos Selos de Certificação, o OCE (Emissor) deverá utilizar um esquema que indique quais atributos as credenciais irão conter. Como ainda não existem esquemas na blockchain, o OCE começa criando um esquema que contém os atributos "numero", "fazenda", "orgaoCertificador", "norma", "safra". Ao publicar o esquema na blockchain, o OCE utiliza seu DID para submeter a transação, tal como mostra a Figura 40, e nomeia o esquema de "selo\_de\_certificacao".

Após a criação do esquema, o OCE procede a criação da definição da credencial (Figura 41), que especifica o esquema e as chaves criptográficas que o Emissor irá utilizar na emissão de credenciais.

### Submit Transaction

Type \* Operation \*  
**Write** **Schema**

DID \*  
**did:mybc:Th7MpTaRZVRyNPiabds81Y**

Name \* Version \*  
**selo\_de\_certificacao** **1.0.0**

Attributes	
numero	✎ ✕
fazenda	✎ ✕
orgaoCertificador	✎ ✕
norma	✎ ✕
safra	✎ ✕

ADD

SUBMIT

### Transaction Result

```

{
  "ver": "1.0",
  "id": "schema:mybc:did:mybc:Th7MpTaRZVRyNPiabds81Y:2:selo_
  "name": "selo_de_certificacao",
  "version": "1.0.0",
  "attrNames": [
    "numero",
    "orgaoCertificador",
    "safra",
    "fazenda",
    "norma"
  ],
  "seqNo": null
}

```

Figura 40 – Submissão do esquema "selo\_de\_certificacao" para a blockchain

### Submit Transaction

Type \* Operation \*  
**Write** **Credential Definition**

Schema ID \*  
**schema:mybc:did:mybc:Th7MpTaRZVRyNPiabds81Y:2:cart**

DID \* Revocable \*  
**did:mybc:Th7MpTaRZVRyNPiabds81Y:2:cart** **Yes**

SUBMIT

### Transaction Result

```

{
  "ver": "1.0",
  "id": "credential:mybc:did:mybc:Th7MpTaRZVRyNPiabds81Y:3:CL:187:19a53e88-b20e-4bea-9ea7-046c6e3c64c9",
  "schemaId": "187",
  "type": "CL",
  "tag": "19a53e88-b20e-4bea-9ea7-046c6e3c64c9",
  "value": {
    "primary": {
      "m": "958299416961674097648295238951130462469299939066975743557477914556086910573152552263299944208862936711418922314242",
      "s": "456055975965404959126432532166817817368398784295266671326063045573236862724506121869934352636312673454910168057463",
      "r": {
        "master_secret": "65150234713106736453561522912301179638433908893749649829272394218919584844890649773562739370508933901"
      },
      "rev": "92135482476114996559405404234626243397693349177919816229457968909849074823074140559318011780920564148149438878",
      "z": "242893929616243899435764625266610664228477228973436296682542516063989759979281124317783061801274598336494770483556"
    },
    "revocation": {
      "hg": "1 3f07f33d1616612EEC189251895E9AF6FECF6A8B5F457A50775C9557116637F 1 16E8B223443679386A71F67A551FF0A424806DEF4F54",
      "g_dash": "1 0AF2052A81D7BC2B639C77919E2BEE80F80C6580940E672568E8E5C2C39085B 1 169A4182288C396D209084A03D2E47C87196A055D",
      "h": "1 0427C1F1324AC55158039C0303E7C181C7209057F96E1895A0F1F9ACA1631B82 1 0621091C9AD7688D06004153697F4A66578CC49089515F9",
      "h0": "1 008E67E5E4A8297DF65A74792875EB840544FD625300F688F797862248219 1 00DF1A60468E7EA4AA2890850314C41A35F3FC0EC15D6E",
      "h1": "1 224C03801381331E187DF40F995F10AC404A3E9145422F053909C1F1D992E85 1 0099762E85ABE9A9A42DA2AF8E1EE6981863F390A85",
      "h2": "1 0E97538C29045F409624148100A7C873080937AFAC320C4278F10F33315684 1 1B2AF3F081F07894AC534800CE4C0705D2475087094",
      "h11de": "1 15DF1956C7E2BDB086F054FDEE82F168B0721B4454A7B33D25237898E8A4EFD4 1 22568E109AC48181A920D318178928B29E8F239F",
      "h_cap": "1 1A862B2FDD845276CD1C880DE4F480746E9980F97D3340638726E19A9192E5C 1 0C07DBAC8260D387C4B00F6C5C7F13D685C3797",
      "u": "1 161FB1A04BDC8E3983A83498AE4D7D66A4C27520A6BF25379D1D86664566 1 23DE3096C22A0F83895F087322323EC21C34D68AD65F",
      "pk": "1 14E938C95148385451268D0651EBABC98A84D5E8A67AE0C9FB988AAAF89FEF 1 0216CDB88AF862DC0EC22E3D01E6118340E9206776C04",
      "y": "1 14466684774FE84C9D8E5C6D5B94C11EE9067C7756947B53F787408CE8F46E 1 0381370C692F4DFF8308FA88C1D5D1CC3CF3EFC5995"
    }
  },
  "schemaId_long": "schema:mybc:did:mybc:Th7MpTaRZVRyNPiabds81Y:2:cartao_de_identificacao:1.0.0"
}

```

Figura 41 – Submissão da definição de uma credencial para a blockchain

## D.4 CRIAÇÃO DE CONEXÕES

Após a base de todo o sistema estar preparada, resta apenas que as entidades comuniquem entre si e compartilhem as informações desejadas. Para esta comunicação ser possível, é necessário estabelecer conexões seguras entre as entidades intervenientes, tal como é explicado no Capítulo 2, Seção 2.3. No COTTONTRUST a gestão de todas as conexões é feita através de uma página como a ilustrada na

Figura 42.

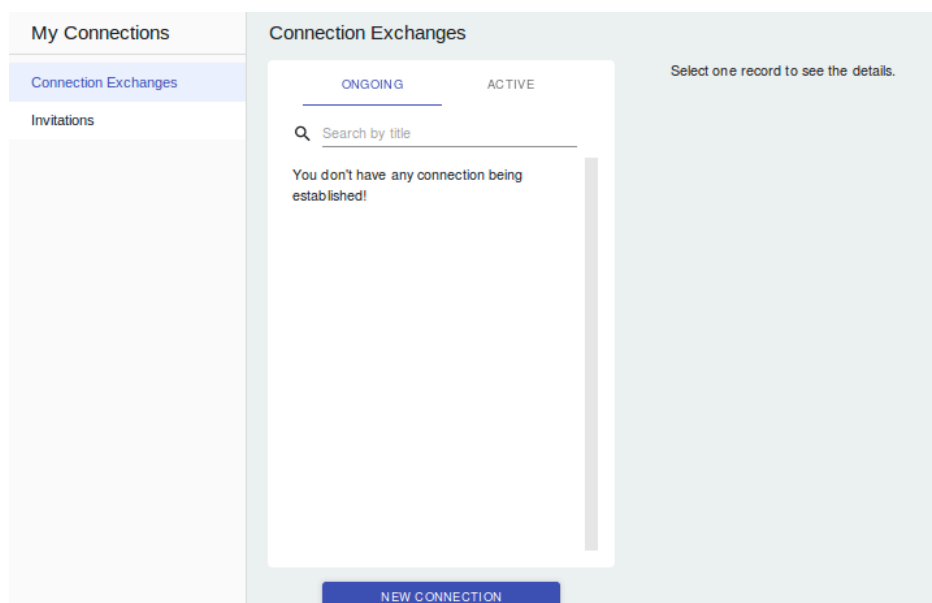


Figura 42 – Página de gestão de conexões

Neste caso de uso, tanto o OCE como o CMI pretendem disponibilizar serviços que outras entidades (*e.g.* o FAD) possam utilizar. Deste modo, o OCE e o CMI irão criar convites, disponibilizando-os eventualmente em algum local acessível (*i.e.* QRCode no *website* ou nos respectivos estabelecimentos físicos ou cartão de visitas). Por sua vez, o FAD irá aceitar cada um desses convites de maneira a estabelecer uma conexão individual com cada um deles. A Figura 43 mostra a criação dos convites de conexão do OCE e do CMI, respectivamente.

**Create Invitation**

Alias\*  
Orgão Certificador

---

Multuse      Public  
Yes            Yes

did  
did:mybc:Th7MpTaRZVRYnPlabds81Y

CREATE INVITATION

**Create Invitation**

Alias\*  
Comprador do Mercado Internacional

---

Multuse      Public  
Yes            Yes

did  
did:mybc:EbP4aYNeTHL6q385GuVpRV

CREATE INVITATION

(a) Criação do convite (OCE)

(b) Criação do convite (CMI)

Figura 43 – Criação do convite de conexão

Durante a criação dos convites, as entidades podem escolher se o convite será utilizado apenas para o estabelecimento de uma conexão ou de múltiplas con-

xões. Independentemente da escolha, estas entidades poderão a qualquer momento desativar ou eliminar o convite, rejeitando assim qualquer tentativa de contato a partir desse momento. A Figura 44 mostra a página através da qual o OCE pode gerir todos os convites que criou.

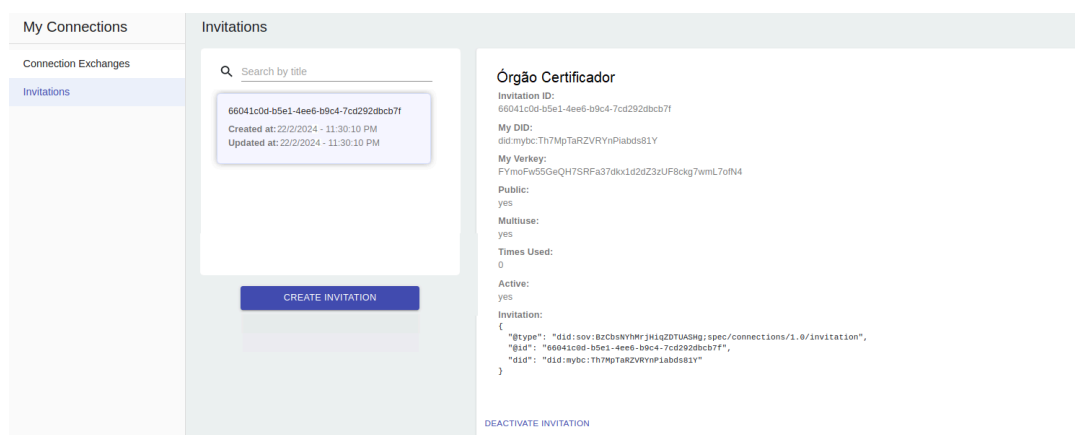
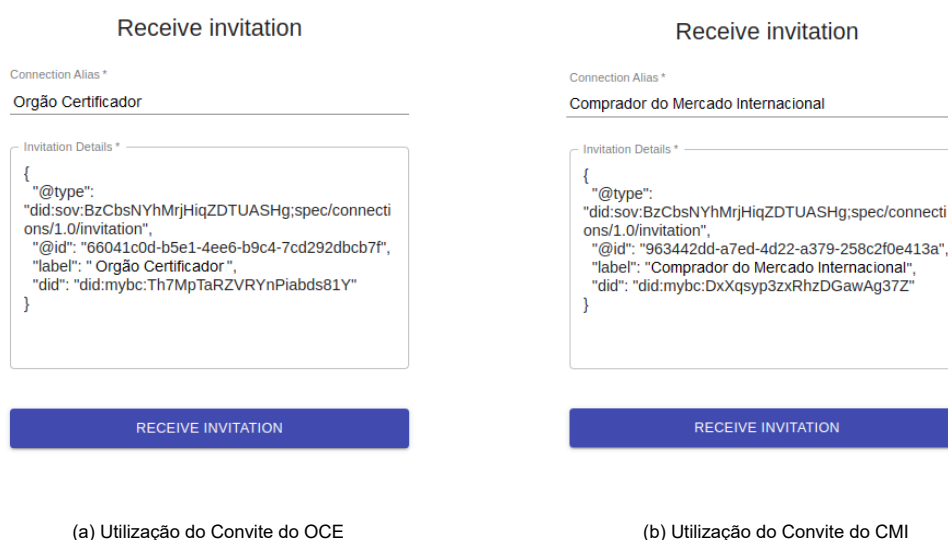


Figura 44 – Página de gestão de conexões - Convites

O próximo passo será disponibilizar estes convites para que outras entidades sejam capazes de os adquirir. Por questões de simplicidade, este exemplo assume que o convite é enviado diretamente ao FAD em formato JSON. Após receber ambos os convites, o FAD procede a importação dos mesmos através da página de gestão de conexões. A Figura 45 mostra a utilização dos convites do OCE e do CMI, respectivamente.



(a) Utilização do Convite do OCE

(b) Utilização do Convite do CMI

Figura 45 – Utilização de convites

Devido a semelhança no estabelecimento de conexões, apenas será demonstrado o processo de estabelecimento de uma conexão entre o FAD e o OCE. Contudo, é necessário efetuar o mesmo processo entre o FAD e o CMI de modo a que ambos possam comunicar entre si. Após utilizar o convite que recebeu do OCE, o FAD poderá optar por aceitá-lo ou rejeitá-lo. Se optar por aceitar o convite, irá efetuar um pedido de conexão ao OCE que, por sua vez, ao receber o pedido do FAD, poderá também aceitá-lo ou rejeitá-lo. Se o OCE optar por aceitar o pedido do FAD, o estabelecimento da conexão será concluído com sucesso e as duas partes poderão comunicar entre si. A Figura 46 mostra novamente a página de gestão de conexões do OCE, na qual é possível verificar que possui uma nova conexão com o FAD no estado ativo.

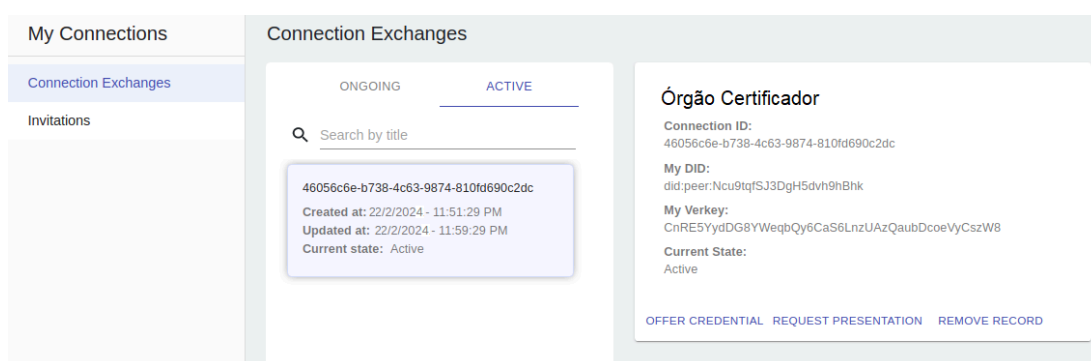


Figura 46 – Conexão ativa entre o OCE e o FAD

## D.5 EMISSÃO DE UMA CREDENCIAL VERIFICÁVEL

Após a conexão entre o FAD e o OCE estar estabelecida, o OCE poderá emitir credenciais verificáveis sobre o FAD. Para iniciar o processo de emissão da credencial destinada ao FAD, o OCE pode fazê-lo por meio da página de gestão de emissão de credenciais ilustrada na Figura 47.

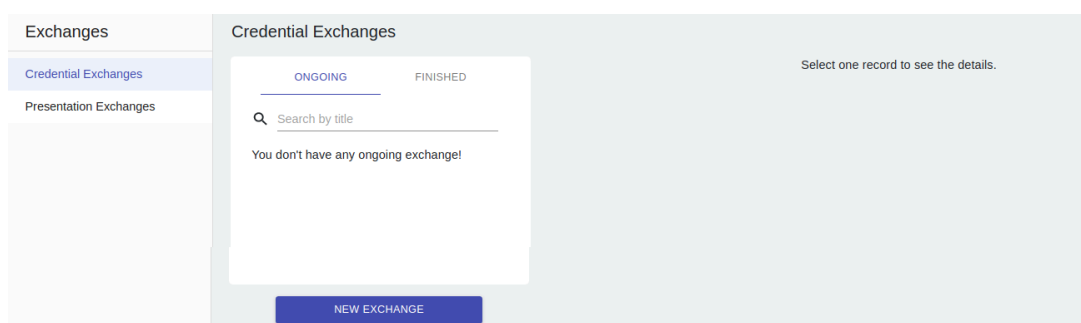


Figura 47 – Página de gestão da emissão de credenciais

Ao clicar no botão para iniciar o processo de emissão de uma nova credencial, é possível iniciar o processo de duas formas: (i) O FAD pode propor ao Emissor

a emissão de uma credencial específica; (ii) O OCE pode oferecer ao FAD uma credencial. Neste caso, o OCE irá iniciar o processo, ofertando uma credencial ao FAD por meio da conexão que ambos estabeleceram e, para tanto, preenche o formulário de acordo com o exemplo ilustrado na Figura 48.

The figure shows three sequential screenshots of the 'Offer Credential' form, illustrating the progress of the process:

- First Screenshot:** Shows the 'General Information' step (1) completed. The form includes:
  - Connection \*: Órgão Certificador
  - Credential Definition ID \*: creddef:mybc:did:mybc:Th7MpTaRZVRYnPiabds8...
  - Comment: Oferta de uma credencial verificável
  - A 'NEXT' button is visible at the bottom right.
- Second Screenshot:** Shows the 'Recipient Attributes' step (2) completed. The form includes:
  - Número: 897.8765.998822
  - Fazenda: Fazenda Terra Santa
  - Safra: 2023/2024
  - Órgão Certificador: GeneZOs Certificações
  - Norma: ABR\_0066BA\_23/24
  - 'BACK' and 'NEXT' buttons are visible at the bottom.
- Third Screenshot:** Shows the 'Confirm Information' step (3) completed. The form displays:
  - Connection: Órgão Certificador
  - Connection ID: 46050c0e-b738-4c63-9874-810fd690c2dc
  - Credential Definition ID: creddef:mybc:did:mybc:Th7MpTaRZVRYnPiabds81Y:3.CL:187:19a53e80-b20e-4bea-9ea7-046c6e3c64c9
  - Schema ID: Th7MpTaRZVRYnPiabds81Y:2:selo\_de\_certificacao:1.0.0
  - Comment: Oferta de uma credencial verificável
  - 'BACK' and 'CONFIRM' buttons are visible at the bottom.

Figura 48 – Formulário de emissão de uma credencial

Na figura apresentada é possível observar que o OCE selecionou a conexão que estabeleceu com o FAD, selecionou o identificador da definição da credencial que criou anteriormente, e inseriu o valor de cada um dos atributos presentes no esquema sob o qual a definição da credencial se baseia. Após confirmar, a oferta da credencial é enviada ao FAD e ambos poderão acompanhar o processo de emissão da credencial por meio da página de gestão da emissão de credenciais de suas respectivas carteiras digitais.

Ao receber a oferta do OCE, o FAD poderá ver os seus detalhes e optar por aceitá-la ou rejeitá-la. Caso decida aceitar, será enviado um pedido de emissão de credencial ao OCE, baseado na oferta que este enviou inicialmente. Assim que o OCE aceitar o pedido recebido, este irá emitir uma nova credencial e enviá-la ao FAD, finalizando o processo. Ao receber a credencial, o FAD irá armazená-la na carteira digital, tal como mostra a Figura 49.

## D.6 APRESENTAÇÃO DE UMA PROVA

Em qualquer momento, o CMI pode desejar confirmar a autenticidade do selo de certificação do FAD. Para tal, deverá indicar a sua intenção ao FAD, por meio de um pedido. Quando receber o pedido, o FAD deverá criar uma apresentação verificável com os atributos requisitados e fornecer essa apresentação ao CMI. Para iniciar um

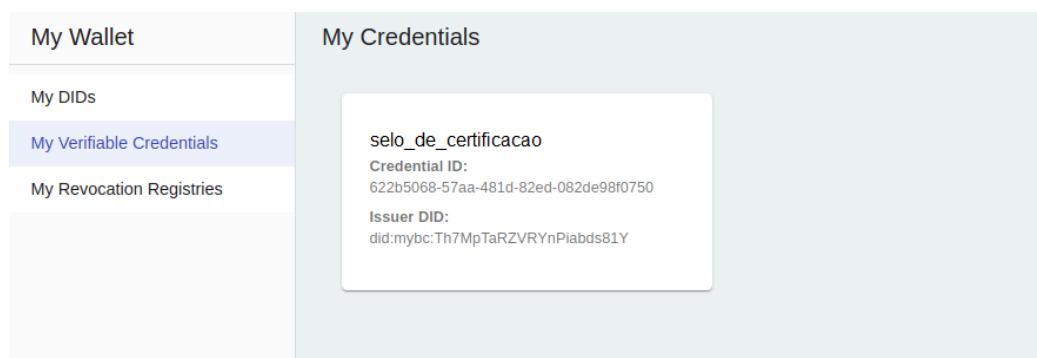


Figura 49 – Página de gestão de credenciais do FAD

novo pedido de apresentação de prova, o CMI pode iniciar este processo através da página de gestão de apresentações de provas, ilustrada na Figura 50.

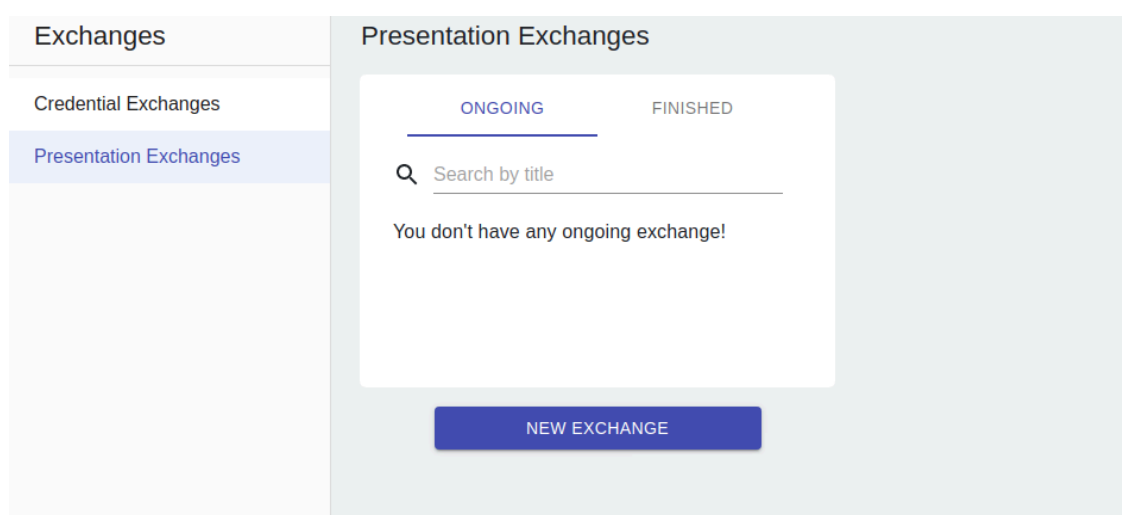


Figura 50 – Página de gestão de apresentações de provas

Com o objetivo de validar se o selo de certificação do FAD é autêntico, o CMI cria um pedido de apresentação de prova que visa obter provas criptograficamente válidas de que o FAD possui os atributos necessários. A Figura 51 mostra o formulário preenchido pelo CMI para a criação de um pedido de prova, no qual é possível verificar que o CMI pretende obter uma prova de que todos os atributos requisitados sejam válidos e não tenham sido revogados. A figura mostra ainda a indicação de que o CMI apenas aceita atributos emitidos pelo OCE, através da inserção do DID que o OCE associou à definição da credencial, e que se baseiem no esquema criado pelo mesmo na Seção D.3.

Semelhante a criação de uma oferta para a emissão de uma credencial, após o CMI enviar o pedido de apresentação da prova, serão criados registros que indicam o estado do processo, tal como mostram as Figuras 52 e 53.

### Request Presentation

Connection \*  
Comprador do Mercado Internacional

Proof Request Name  
Prova de autenticidade do selo de certificação

Non Revoked (From) 27/02/2021 12:27:26 AM  
Non Revoked (To) 27/02/2026 12:27:26 AM

Attributes	
orgaoCertificador	<input type="checkbox"/> <input type="checkbox"/>
safra	<input type="checkbox"/> <input type="checkbox"/>
fazenda	<input type="checkbox"/> <input type="checkbox"/>
norma	<input type="checkbox"/> <input type="checkbox"/>

Predicates	
	<input type="checkbox"/> <input type="checkbox"/>

Figura 51 – Formulário de pedido de prova

Exchanges

- Credential Exchanges
- Presentation Exchanges**

#### Presentation Exchanges

ONGOING
FINISHED

Search by title

dc3719f1-046e-465c-be0b-9244583ecc33

Created at: 22/2/2024 - 11:30:10 PM

Updated at: 22/2/2024 - 11:30:10 PM

Current state: Request Sent

Current State:  
Request Sent

Presentation Proposal:  
\*\*

Presentation Request:

```
{
  "non_revoked": {
    "from": "1612657646",
    "to": "1612657646"
  },
  "requested_attributes": {
    "attributes": {
      "non_revoked": {
        "from": "1612657646",
        "to": "1612657646"
      },
      "restrictions": [
        {
          "schema_id": "schema:mybc:dId:mybc:Th7pTaR2VRyNpIabds81y:2:",
          "issuer_did": "did:mybc:Th7pTaR2VRyNpIabds81y"
        }
      ]
    }
  },
  "requested_predicates": {
    "predicates": {
      "non_revoked": {
        "from": "1612657646",
        "to": "1612657646"
      },
      "restrictions": [
        {
          "schema_id": "schema:mybc:dId:mybc:Th7pTaR2VRyNpIabds81y:2:",
          "issuer_did": "did:mybc:Th7pTaR2VRyNpIabds81y"
        }
      ]
    }
  },
  "version": "1.0",
  "ver": "2.0",
  "date": "1612656256",
}
```

Figura 52 – Página de gestão de apresentações de provas do CMI

Ao receber o pedido de apresentação de prova do CMI, o FAD pode aceitar ou rejeitar esse pedido. Caso opte por aceitar, o FAD poderá escolher de quais credenciais pretende seleccionar os atributos para construir a apresentação da prova. Se o FAD desejar, poderá agregar atributos de diferentes credenciais numa única apresentação verificável desde que cada atributo individual cumpra as restrições impostas no pedido enviado pelo CMI.

Neste caso de uso o FAD possui uma única credencial pelo que apenas poderá escolher os atributos dessa credencial durante a construção da prova. Ao receber

Exchanges

Credential Exchanges

Presentation Exchanges

ONGOING FINISHED

Search by title

dcb7191f-046e-465c-be0b-9244583ecc33  
Created at: 22/3/2024 - 11:30:10 PM  
Updated at: 22/3/2024 - 11:30:10 PM  
Current state: Request Sent

NEW EXCHANGE

Record ID: f9807d41-25b4-4ff-87c1-deb49535504b  
Connection ID: 5039e3e8-2cc9-493e-b487-9bee9ea7211d  
Initiator: external  
Role: prover  
Thread ID: 2628f904-9faf-4822-b88f-2620990f850e  
Current State: Request Received  
Presentation Proposal: ""

Presentation Request:

```
{
  "non_revoked": {
    "from": 1612657646,
    "to": 1612657646
  },
  "requested_attributes": {
    "attributes": {
      "non_revoked": {
        "from": 1612657646,
        "to": 1612657646
      },
      "restrictions": [
        {
          "schema_id": "schema:mybc:did:mybc:Th7MPTaRZVRYPiabds81Y:2:1",
          "issuer_did": "did:mybc:Th7MPTaRZVRYPiabds81Y"
        }
      ]
    }
  },
  "requested_predicates": {
    "predicates": {
      "non_revoked": {
        "from": 1612657646,
        "to": 1612657646
      }
    }
  }
}
```

ACCEPT REQUEST REJECT REQUEST REMOVE RECORD

Figura 53 – Página de gestão de apresentações de provas do FAD

a apresentação criada pelo FAD, o CMI poderá verificar a validade da mesma, como é possível observar na Figura 54. Após verificar a validade da prova, o CMI irá obter a indicação de que a prova é válida dentro dos parâmetros estabelecidos.

Exchanges

Credential Exchanges

Presentation Exchanges

ONGOING FINISHED

Search by title

dcb7191f-046e-465c-be0b-9244583ecc33  
Created at: 22/3/2024 - 11:30:10 PM  
Updated at: 22/3/2024 - 11:34:10 PM  
Current state: Completed

NEW EXCHANGE

Current State: Request Sent  
Presentation Proposal: ""

Presentation Request:

```
{
  "non_revoked": {
    "from": 1612657646,
    "to": 1612657646
  },
  "requested_attributes": {
    "attribute1": {
      "non_revoked": {
        "from": 1612657646,
        "to": 1612657646
      },
      "restrictions": [
        {
          "schema_id": "schema:mybc:did:mybc:Th7MPTaRZVRYPiabds81Y:2:1",
          "issuer_did": "did:mybc:Th7MPTaRZVRYPiabds81Y"
        }
      ]
    }
  },
  "requested_predicates": {
    "predicates": {
      "non_revoked": {
        "from": 1612657646,
        "to": 1612657646
      }
    }
  }
}
```

VERIFY PRESENTATION

Figura 54 – CMI verifica a validade da prova