UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Luca Fachini Campelli

Protocolo de diploma Digital Auto-Soberano com Retrocompatibilidade Tecnológica focado na Realidade Brasileira

Florianópolis
2022

Luca Fachini Campelli

Protocolo de diploma Digital Auto-Soberano com Retrocompatibilidade Tecnológica focado na Realidade Brasileira

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação para a obtenção do título de mestre em Ciências da Computação.
Orientador: Prof. Jean Everson Martina, Dr.

Florianópolis
2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Campelli, Luca
Protocolo de Diploma Digital Auto-Soberano com Retrocompatibilidade Tecnológica focado na Realidade Brasileira / Luca Campelli ; orientador, Jean Everson Martina, 2022.
62 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós-Graduação em Ciência da Computação, Florianópolis, 2022.

Inclui referências.

1. Ciência da Computação. 2. Documentos Digitais. 3. Blockchain. 4. Self-Sovereign Identity. I. Everson Martina, Jean. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

Luca Fachini Campelli

Protocolo de diploma Digital Auto-Soberano com Retrocompatibilidade Tecnológica focado na Realidade Brasileira

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Profa. Thais Bardini Idalino
Universidade Federal de Santa Catarina

Prof. Marco Aurelio Amaral Henriques
Unicamp

Martín Augusto Gagliotti Vigil
Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Ciências da Computação.

Documento assinado digitalmente
PATRICIA DELLA MEA PLENTZ
Data: 16/10/2022 15:57:30-0300
CPF: ***.243.700-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Patricia Della Mea Plentz
Coordenadora do Programa

Documento assinado digitalmente
Jean Everson Martina
Data: 17/10/2022 11:33:54-0300
CPF: ***.355.939-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Jean Everson Martina, Dr.
Orientador

Florianópolis, 2022.

Este trabalho é dedicado à todos aqueles que me empurraram
quando eu estava atolado.

AGRADECIMENTOS

Agradeço a todos que botaram fé em mim.

“O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001

Não me responsabilizo pelo que disse antes, pois na época eu era mais jovem
e mais tolo, e agora sou mais velho e menos tolo. - O autor

RESUMO

Estudos revelam que o processo de emissão de diplomas de Conclusão de Curso no Brasil pode ser complexo, demorado e vulnerável a ataques. Em 2018, uma proposta do Ministério da Educação (MEC) trouxe ao Brasil o diploma Digital, uma solução em formato XML assinado digitalmente, que tem como um de seus objetivos a redução dos casos de diplomas falsos. Entretanto, esta solução não abrange o acompanhamento do histórico escolar do aluno, etapa na qual também podem ocorrer fraudes. Mesmo soluções que utilizam tecnologias inovadoras, como a blockchain, não contemplam toda a jornada do estudante ou não apresentam de maneira contundente um caminho viável para o salto tecnológico. Neste trabalho, foi feita uma revisão bibliográfica da literatura, trazendo idéias e trabalhos que tentam resolver este mesmo problema. Será então apresentado um protocolo de emissão de créditos e diplomas inteiramente baseado na plataforma Hyperledger Indy, uma tecnologia blockchain derivada da iniciativa Hyperledger e com foco em SSI (Self-Sovereign Identity). O protocolo proposto provê validade e rastreabilidade mesmo para diplomas anteriormente emitidos com tecnologias legadas.

Palavras-chave: Self-Sovereign Identity. diploma Digital. blockchain. Hyperledger Indy.

ABSTRACT

Studies reveal that the process of issuing degree certificates in Brazil has the potential to be complex, time-consuming, and vulnerable to attacks. In this context, in 2018, the Ministry of Education proposed a digitally signed degree certificate in XML format. One of their goals was to reduce cases of false degree certificates. However, their solution does not cover the monitoring of the student's academic records, a stage in which fraud may also occur. Furthermore, even solutions that use innovative technologies, such as blockchain, do not contemplate the student's entire journey and do not present a convincing way for the technological leap. In this article a bibliographical review was made, bringing ideas and articles that attempted to solve the same problem. I then proposes a protocol for issuing credits and degree certificates based on the Hyperledger Indy platform, a blockchain technology derived from the Hyperledger initiative and focused on SSI (Self-Sovereign Identity). The proposed protocol provides validity and traceability even for previous degree certificates issued with other legacy technologies.

Keywords: Self-Sovereign Identity. Digital diploma. blockchain. Hyperledger Indy.

LISTA DE ILUSTRAÇÕES

LISTA DE ALGORITMOS

LISTA DE ABREVIAÇÕES

- DID - Decentralized Identifier
- HEI - Higher Education Institution / Instituição de Ensino Superior
- RA - Regulation Authority / autoridade Reguladora
- PAD - Personal Authentication Device / Dispositivo de Autenticação Pessoal
- SSI - Self Sovereign Identity / Identidade Auto Soberana
- MIT - Massachussets Institute of Technology
- ICP-Brasil - Infraestrututra de Chaves Públicas do Brasil
- ZKP - Zero Knowledge Proof / Provas de Conhecimento Zero
- JSON - JavaScript Object Notation
- Dapp - Decentralized Aplication / Aplicativo Descentralizado
- SDK - Software Development Kit / Kit de Desenvolvimento de Software
- KYC - Know your customer / Conheça Seu Cliente
- CED - Credencial de Emissão de Diploma
- DIP - Credencial de Diploma
- CCD - Credencial de Conclusão de Disciplina

SUMÁRIO

1 INTRODUÇÃO

Sabe-se que a identidade de uma pessoa pode ser aferida por sua documentação. Os documentos obtidos ao longo de sua vida podem descrever suas conquistas e qualidades, além de é claro, sua identidade. Por exemplo, no meio acadêmico brasileiro, ao longo de sua jornada escolar, o estudante irá acumular uma grande variedade de diplomas e certificações que demonstrarão suas conquistas. Documentos estes que, em sua maioria, serão emitidos em papel, timbrados e assinados manualmente (PEREIRA et al., 2015). Além disso, mecanismos como o uso de marcas d'água e papel moeda são utilizados para atribuir veracidade e validade a estes documentos. Entretanto, na realidade, percebe-se que estes artifícios não são suficientes para evitar as falsificações, como é possível identificar em inúmeras reportagens da mídia tradicional (GLOBO G1 CE, 2021).

Neste contexto, na literatura e na indústria, pode-se encontrar diferentes propostas para atribuir maior segurança e privacidade aos documentos emitidos no contexto do ensino. Por exemplo, em 2018, o Ministério da Educação do Brasil (MEC) iniciou um projeto com a Portaria nº330 de 5 de Abril de 2018 (MINISTÉRIO DA EDUCAÇÃO BRASILEIRO, 2018), para implementar o *diploma Digital* em território nacional. Este diploma digital, é um arquivo XML assinado digitalmente com chaves criptográficas da Estrutura de Chaves Públicas do Brasil (ICP-BRASIL) e tem como um de seus principais objetivos a redução das fraudes, que regularmente ocorrem com os documentos tradicionais. Esta assinatura digital dá ao documento um carimbo de tempo e validade jurídica (GOVERNO BRASILEIRO, 2001).

Também, na literatura, pode-se encontrar outras abordagens que buscam adicionar características de temporalidade, e verificabilidade a estes documentos através da adoção da tecnologia blockchain. Esta tecnologia é uma estrutura que organiza os dados em uma lista de blocos encadeada, onde cada bloco possui um conjunto de dados, como arquivos ou transações de valores, e um resumo criptográfico calculado a partir do conteúdo do bloco anterior. Um exemplo desse tipo de abordagem, é a iniciativa do *Massachusetts Institute of Technology* (MIT), denominada *Blockcerts*, que adota a blockchain para o armazenamento de resumos criptográficos de documentos digitais. Esse sistema já está em uso e alunos do MIT podem escolher se querem receber seu diploma de conclusão em meio físico ou digital, através de um aplicativo para aparelhos móveis (MIT MEDIA LABS, 2016).

Em 2014, a Universidade de Nicosia foi a primeira instituição de ensino a registrar certificados de conclusão de curso na blockchain. Como parte de um curso específico sobre a tecnologia, a instituição emitiu documentos digitais e armazenou seus resumos criptográficos em uma blockchain pública, meio no qual qualquer usuário pode realizar consultas e emitir transações, permitindo que os alunos que atenderam ao curso pudessem verificar seus certificados, sem depender da universidade (WONG, 2014).

Além dos trabalhos citados, outros projetos e pesquisas propõem o armazenamento de informações em uma blockchain a fim de torná-las verificáveis e resistentes a modificações. Este é o caso da proposta de (GHAZALI; SALEH, 2018) que armazena na blockchain uma

transação (entre a instituição de ensino e o aluno) cujo conteúdo é o resumo criptográfico do documento de conclusão. Outros como (BRUNNER; KNIRSCH; ENGEL, 2019) utilizam árvores de Merkle para que vários documentos possam ser publicados na blockchain em uma só transação. (YEH, 2018) foca em armazenar e recuperar o documento ao utilizar um QR code e dividindo-o em partes que são armazenadas em locais diferentes. O trabalho de (PALMA et al., 2019) traz o uso de smart contracts para a automatização do sistema e armazenamento do histórico do aluno e consequente verificação e emissão do diploma. Demais trabalhos procuram focar em outros aspectos do processo, como (VIDAL; GOUVEIA; SOARES, 2020b) que foca em estudar a revogação de um documento emitido.

O trabalho de (PALMA et al., 2020) foi iniciado com o intuito de trazer uma forma de usar smart contracts para gerenciar e armazenar os registros acadêmicos do aluno ao longo de sua carreira acadêmica. Este trabalho foi desenvolvido até que se tornou parte de um projeto público do Ministério da Educação Brasileiro (BRASILEIRO, 2021).

Mesmo com estas inovações na forma de armazenamento e no processo de emissão, em um cenário onde seja necessário compartilhar estes documentos, a verificação da validade dos mesmos pode ser difícil ou pouco intuitiva e, por vezes, gerar cópias fora do controle dos indivíduos a que se referem. Um destes casos é na aplicação para um emprego. Para isso, um indivíduo que se gradua em uma instituição de ensino superior precisa provar para futuros empregadores suas conquistas acadêmicas. As formas de realizar esta verificação exigem o envio das informações do indivíduo para os empregadores, o que não garante a veracidade dos documentos, já que diversos tipos de documentos podem ser forjados e replicados com facilidade e ainda assim, uma cópia física ou digital dos dados terá sido enviada, que pode ser utilizada para extrair informações pessoais do indivíduo, ou clonar seu documento. Neste sentido, uma solução para garantir maior segurança e privacidade dos dados de uma pessoa é o SSI ou *Self Sovereign Identity*. Este conceito define que a identidade de um indivíduo é de sua inteira responsabilidade e posse (LóPEZ, 2020). Segundo (ALLEN, 2016), pode-se elencar dez pontos que descrevem SSI:

- **Existência** - A existência do indivíduo deve ser única, e não somente digital.
- **Controle** - Indivíduos devem ter o controle sobre suas identidades - Os usuários devem ter o poder de atualizá-las, referenciá-las e até escondê-las, além de escolher o quão públicas elas são.
- **Acesso** - O indivíduo deve ter acesso total a sua identidade - Deve ser possível ter acesso a todas as afirmações e dados sobre a própria identidade, sem ofuscamento.
- **Transparência** - Sistemas e algoritmos utilizados devem ser transparentes.
- **Persistência** - Identidades devem durar por um logo tempo - Devem se manter válidas até que se tornem desatualizadas por sistemas mais novos.

- **Portabilidade** - Informações e serviços de identidade devem se manter transportáveis - Identidades devem poder ser utilizadas em qualquer sistema, e não serem retidas por apenas um provedor de identidades terceiro.
- **Interoperabilidade** - Identidades devem ser o mais amplamente utilizáveis quanto possível - Uma identidade deve ser aceita na maior quantidade de serviços possível.
- **Consentimento** - Indivíduos devem consentir o uso de suas identidades - A identidade em si funciona sendo compartilhada, e mesmo que outros indivíduos possam fazer afirmações sobre uma identidade, o indivíduo ainda deve dar consentimento para que elas se tornem válidas.
- **Minimização** - Apenas o mínimo necessário de informação deve ser compartilhado - Se uma verificação requerer a prova de maioridade, não se é necessário compartilhar a idade exata ou data completa de nascimento.
- **Proteção** - Os direitos dos usuários devem ser protegidos - Conflitos devem ser resolvidos de forma que não prejudiquem os direitos do usuário.

1.1 CONTEXTUALIZAÇÃO DO PROBLEMA

Poucas pesquisas na literatura utilizam SSI como parte fundamental de suas propostas de emissão de diplomas de conclusão de cursos e créditos acadêmicos. Alguns trabalhos que adotam a blockchain se aproximam do conceito, porém falham por não cumprir com um ou outro dos dez pontos citados anteriormente (DURANT; TRACHY, 2017)(PETRE; PAQUE; LEJEUNE, 2019)(YEH, 2018). Por exemplo, uma das tecnologias blockchain trazidas nesta pesquisa, a Hyperledger Indy, possui em seus exemplos práticos um caso onde um diploma é emitido por uma instituição e atribuído à um usuário. Porém, por se tratar de um exemplo da documentação, é apresentado de forma genérica, além de não levar em conta legislações específicas ou documentos legados gerados fora do sistema.

1.2 OBJETIVO GERAL

O objetivo geral deste trabalho é impulsionar o salto tecnológico através da integração com processos já existentes de emissão de diplomas e registro de créditos. Para tanto, adotou-se como base o protocolo do Hyperledger Indy (HYPERLEDGER FOUNDATION, 2018), pois este já é utilizado por grandes iniciativas, como é o caso do Sovrin (THE SOVRIN FOUNDATION, 2018) e possui uma comunidade ativa de desenvolvedores.

1.2.1 Objetivos específicos

Os objetivos específicos deste trabalho são os seguintes:

- Propor um protocolo, onde todo o processo de emissão do diploma seja considerado, desde os dados de histórico, até a emissão e utilização do documento na prática.
- O protocolo deve levar em conta a existência de sistemas legados de documentação, permitindo uma transição entre os sistemas.
- Construir um protótipo de um sistema baseado no protocolo proposto.

1.3 METODOLOGIA

Neste capítulo será explicada a metodologia utilizada para a elaboração da pesquisa. No início do projeto, foi feita uma revisão sistemática da literatura, para se buscar os caminhos de inovação tecnológica e estado da arte. Nesta revisão diversos trabalhos foram encontrados trazendo diversas maneiras de utilizar sistemas de blockchain para o armazenamento de documentos, porém se confirmou que muitos poucos trabalhos pensavam no histórico do aluno em si, ou na retrocompatibilidade tecnológica. Foi então proposto um protocolo de emissão de diplomas Digitais de Conclusão de Curso em um ambiente Self-Sovereign Identity, levando em conta a atual forma de emissão de diplomas. Depois, um protótipo funcional com base no protocolo foi construído, a fim de analisar sua viabilidade, seus prós e contras, e compará-lo aos métodos atuais de emissão de diplomas em meios digitais encontrados na revisão sistemática.

1.4 PUBLICAÇÕES DO TRABALHO

Este trabalho foi aceito como um artigo completo no Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg) 2021, com o titulo “Protocolo de diploma Auto-Soberano com Retrocompatibilidade Tecnológica: Uma Solução Adaptada a Realidade Brasileira” e foi pulicado em Outubro de 2021.

1.5 ORGANIZAÇÃO DO TEXTO

O restante deste documento está organizado da seguinte maneira: no capítulo 2 são apresentados conceitos essenciais para a compreensão da proposta. No capítulo 3 é descrito o protocolo de revisão sistemática efetuado e seus resultados. No capítulo 4, apresenta-se o protocolo desenvolvido e são trazidas as contribuições desta pesquisa. fim no capítulo 6 são apresentadas as conclusões e discussões acerca da pesquisa.

2 CONCEITOS PRELIMINARES

Neste capítulo são apresentados os conceitos e tecnologias utilizados no protocolo proposto no capítulo 4. No capítulo 2.1, apresenta-se brevemente uma definição de resumos criptográficos, uma vez que são a base da tecnologia blockchain. Em seguida, no capítulo 2.2, discute-se conceitos introdutórios de blockchain. Por fim, o capítulo 2.3 introduz-se SSI.

2.1 RESUMOS CRIPTOGRÁFICOS

Um resumo criptográfico é uma função cujo objetivo é receber como entrada uma cadeia de tamanho variável de caracteres e retornar uma cadeia de tamanho fixo como mostra a Figura 1, obedecendo certas propriedades como (PRENEEL, 1994):

- **Pré-Imagem**: Dado um resumo criptográfico *h*, deve ser inviável computacionalmente encontrar uma mensagem *m* tal que *h = hash(m)*.
- **Segunda Pré-Imagem ou Colisão Fraca**: Dada uma mensagem *m1*, deve ser computacionalmente inviável encontrar outra mensagem *m2*, tal que *hash(m1) = hash(m2)*.
- **Colisão Forte**: Deve ser computacionalmente inviável encontrar duas mensagens distintas *m1* e *m2*, tal que *hash(m1) = hash(m2)*.

Estas propriedades permitem a verificação de integridade de um dado qualquer, como por exemplo um arquivo de texto *A*. Basta que se tenha conhecimento de *A* e *H(A)*, pois sempre que for necessário conferir se *A* foi alterado, pode-se calcular novamente o seu resumo criptográfico e confrontá-lo com *H(A)* previamente conhecido.

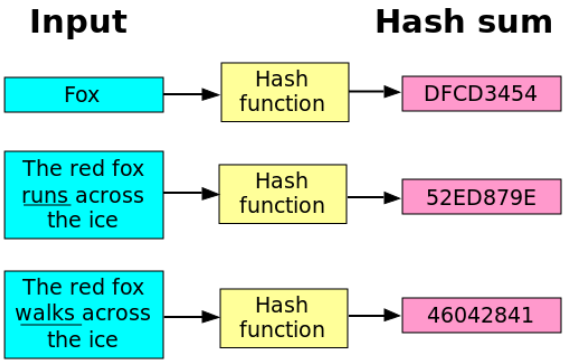

Figura 1 – Demonstração do funcionamento da função de Resumo Criptográfico (DAVIDGOTHBERG, 2005)

2.2 BLOCKCHAIN

Inicialmente descrita por Satoshi Nakamoto, blockchain é uma estrutura de dados distribuída que foi a base para o funcionamento da criptomoeda Bitcoin (NAKAMOTO, 2008). Esta estrutura, apresenta-se como uma lista encadeada e distribuída de blocos, onde um bloco B_i está ligado ao bloco anterior B_{i-1} por meio de um resumo criptográfico gerado a partir do conteúdo do bloco anterior como mostra a Figura 2. A inserção de um bloco na lista se dá por meio da realização de uma prova de trabalho, um desafio matemático, computacionalmente difícil de ser completado, mas de fácil verificação.

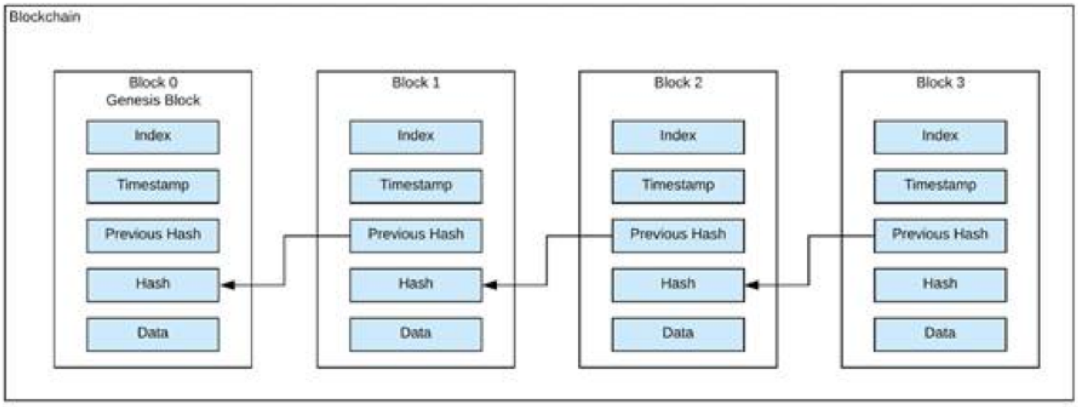

Figura 2 – Demonstração da estrutura dos blocos da blockchain. (DHONGADE, 2019)

A prova de trabalho funciona ao estipular uma condição para que os resumos criptográficos sejam considerados válidos, por exemplo, ter um número específico de "zeros" no início da cadeia, o que exige que um pedaço de informação seja adicionado ao final do bloco, e então seja calculado seu resumo criptográfico. O cálculo deste pedaço de informação é computacionalmente difícil, porém depois de realizado, ele é anexado ao bloco, e portanto a verificação da execução da prova de trabalho é fácil, ao se calcular o resumo criptográfico do bloco com o valor já anexado (JAKOBSSON; JUELS, 1999).

A blockchain é, em geral, um sistema distribuído, onde cada usuário da rede armazena a corrente inteira. Por ser distribuída, pode ocorrer que dois usuários tenham cópias diferentes da corrente e uma das formas utilizadas para resolver este conflito é considerar a corrente mais longa como a corrente válida.

Como a computação de um bloco pode ser demorada (na ordem de minutos no caso do Bitcoin), para modificar um bloco já encadeado, um atacante deve modificar seu conteúdo e calcular o resumo criptográfico de todos os blocos que foram adicionados posteriormente, o que se torna praticamente impossível sem um poder computacional que exceda o poder computacional de mais da metade dos usuários da rede. Por este motivo, um bloco B_i que possua índice i suficientemente grande é considerado imutável, sendo esta uma principal característica dos dados inseridos em uma blockchain.

Em geral, as blockchains podem ter três tipos de acesso: privado, público ou híbrido. Em blockchains públicas, os usuários são anônimos e identificados apenas por um endereço, que

pode ser um resumo criptográfico ou uma chave pública. Assim, estes podem emitir transações e participar da prova de trabalho. As vantagens deste tipo de acesso são que todo trafego na rede é público e verificável, pois qualquer um que tem acesso à rede pode enviar e verificar transações (PILKINGTON, 2016).

Já blockchains privadas exigem que os usuários sejam conhecidos e convidados a participar da geração da cadeia de blocos. Isso ajuda em muitos pontos de segurança, já que como os usuários do sistema são conhecidos, um usuário dá um voto de confiança ao convidar outro para a rede. Normalmente redes privadas são menores, por exigir o convite e conhecimento dos usuários, mas por causa disso, podem ter outras conveniências como diminuição dos custos das transações, e segurança, graças a não anonimização dos usuários. Por fim as blockchains híbridas são a combinação das duas anteriores, podendo operar em parte de forma pública e outra de forma privada, trazendo benefícios dos dois tipos (PILKINGTON, 2016).

Em uma blockchain pública, os usuários não são identificados por seus endereços, não há como ligar o endereço a um indivíduo sem mais informações do que só o endereço. Desta forma um nodo maligno não pode ser corretamente identificado e mesmo que seja bloqueado o endereço, o indivíduo pode continuar a criar novos endereços e entrar novamente na rede. Não só isso, como não é possível descobrir se por traz de um endereço há mesmo uma pessoa. Em um tipo de ataque conhecido como Sybil (DOUCEUR, 2002), um nodo da rede pode assumir mais de uma identidade, e caso consiga ocupar mais de 50% do poder de processamento da rede ele pode controlar o tráfego de blocos, ou somente aprovar blocos com transações inválidas, ou aprovar transações mal-intencionadas. Este tipo de ataque é menos efetivo em blockchains privadas, por terem seus próprios métodos de verificação de blocos e pela não anonimização dos usuários.

O endereço da blockchain pode ser um identificador anônimo do usuário, um número aleatório ou hash, ou um identificador de um usuário conhecido como uma chave pública. Todos estes níveis de identificação podem ser obtidos através do uso de uma Infra-estrutura de Chaves Públicas. No Brasil por exemplo, existe a ICP-Brasil, um órgão que administra a criação e manutenção de certificados digitais, e poderia ser utilizado em conjunto com sistemas de blockchain para o seu funcionamento e credenciamento dos usuários (PALMA et al., 2019).

Além do Bitcoin, vale destacar outras implementações de blockchain como o Ethereum (WOOD et al., 2014) e o conjunto de implementações da Hyperledger (HYPERLEDGER FOUNDATION, 2015). Nestas, uma inovação é a introdução dos smart contracts, pedaços de códigos que existem e executam dentro do contexto da cadeia, possuem endereços próprios e permitem a criação dos aplicativos decentralizados, aplicativos cuja lógica mais complexa se encontra totalmente na blockchain, em formato de smart contracts. (RAVAL, 2016).

Os smart contracts são programas que podem ser desenvolvidos em sua própria linguagem de programação e uma vez implementados, podem funcionar sozinhos de forma autônoma (SZABO, 1997). Sua execução depende de uma transação na blockchain, e ao executar o código nele programado, é possível até que um Smart Contract crie outros smart contracts (MOHANTA; PANDA; JENA, 2018).

2.3 SELF SOVEREIGN IDENTITY

Self-Sovereign Identity (SSI), também conhecida como Identidade Auto-Soberana, é o conceito onde a soberania e responsabilidade sobre a identidade de um indivíduo se encontra com ele mesmo. Diferentemente dos provedores de identidade, os dados e credenciais acerca de um indivíduo se encontram em sua posse, e é ele quem decide quando e quais informações serão compartilhadas (LóPEZ, 2020).

Provedores de identidades podem ser separados em dois tipos, próprios ou terceiros. Provedores próprios são, como o nome já diz, provedores dos próprios serviços. Todo o tipo de website que exija um cadastro para acessar suas funcionalidades, por exemplo, é um provedor de identidade próprio. Provedores terceiros são provedores que autenticam a identidade para outros serviços. Um exemplo deste tipo de provedor é a Google, ou o Facebook, que permitem que serviços de outros websites sejam acessados por meio de seus provedores de identidade. (LóPEZ, 2020).

O foco de SSI é a privacidade do usuário, atribuindo a ele a autoridade sobre sua identidade. Estes poderes incluem quais informações são discorridas, em quais meios e quais permissões sobre estas informações são dadas as outras partes que as recebem. A principal característica de SSI é a responsabilidade sobre as informações. Ou seja, o usuário possui a responsabilidade sobre seus dados, e quaisquer informações que ele compartilhe só serão compartilhadas com o seu consentimento. Em um exemplo, (LóPEZ, 2020) mostra que se poderia até lucrar com a venda de informações, onde um órgão deveria pagar ao usuário para compartilhar suas informações com outras instituições, e isto somente com seu consentimento.

Outro ponto é o fato de que, sob a SSI, apenas o que é necessário ser discorrido é efetivamente conhecido, e por saber exatamente o que é pedido, o usuário pode escolher o que e como compartilhar a informação. Mesmo assim, órgãos governamentais não perderiam sua função. Embora as responsabilidades sobre a identidade caiam sobre o usuário, a emissão de dados válidos e verificáveis se mantém em posse destes órgãos. Todos os dados que são emitidos como credenciais e dados aos usuários são assinados pelas instituições emissoras, e caso sejam descobertos dados fraudulentos, a confiabilidade nessas instituições se encontrará abalada (LóPEZ, 2020).

Neste contexto, outras tecnologias existentes têm uma grande afinidade com SSI e são utilizadas como parte de sua implementação (ALLEN, 2016). Um exemplo é o Zero-Knowledge Proof, ou Provas de Conhecimento Zero, que permitem a criação de afirmações sobre as informações do indivíduo que possam ser inegavelmente provadas verdadeiras, sem necessariamente expor qualquer informação privada (FORTNOW, 1987).

2.4 HYPERLEDGER INDY

Hyperledger Indy é uma iniciativa criada pela Hyperledger Foundation, ele engloba um framework de identidade descentralizada e de uma ledger distribuída (HYPERLEDGER

FOUNDATION, 2018). O Hyperledger Indy é um ramo da arquitetura Hyperledger que foca em identidades descentralizadas. É um projeto com uma comunidade ativa de desenvolvedores e já é utilizado em sistemas existentes como o Sovrin (THE SOVRIN FOUNDATION, 2018). A arquitetura Hyperledger disponibiliza uma Ledger para ser utilizada em desenvolvimento e um framework de desenvolvimento para identidade descentralizada. Neste framework é possível criar as Wallets, ou Carteiras, onde todas as credenciais são armazenadas para um usuário. É possível também declarar e publicar Esquemas / Schemas, Definições / Definitions e Credenciais / Credentials, além de criar os Identificadores Descentralizados / Descentralized Identifiers (DID) que são os endereços aos quais um usuário atrela sua identidade. Um usuário pode possuir mais de um DID, porém um DID só pode ser ligado a usuário. A arquitetura também permite que os usuários possuam papéis, sendo que apenas usuários com papéis elevados podem publicar na ledger e emitir credenciais. Outras capacidades do Hyperledger, por exemplo, são de rotacionar chaves para a carteira, revogação de credenciais por meios de repositórios públicos, e realizar provas de conhecimento zero sobre os dados de uma credencial, além e poder validar as provas.

2.5 ZERO KNOWLEDGE PROOF / PROVAS DE CONHECIMENTO ZERO

Provas de Conhecimento Zero permitem que seja criada uma forma de validar de forma inegável que uma afirmação é verdadeira sem efetivamente expor nenhum dado sensível relativo a pessoa (FORTNOW, 1987). Um exemplo desse fato seria em uma entrada para algum evento que exija uma carteira de identidade ou prova de idade de um frequentador. Neste caso apresentar a carteira de identidade deixa muitos outros dados sensíveis à mostra, como nome da mãe, e data completa de nascimento por exemplo. Uma Prova de Conhecimento Zero poderia neste caso responder que a pessoa possui sim mais que 18 anos sem necessariamente expor sua data de nascimento completa.

2.6 ÁRVORES DE MERKLE

Árvores de Merkle são estruturas de dados em formato de árvore binária onde os nodos folha são resumos criptográficos. Cada nodo acima das folhas é um resumo criptográfico calculado a partir dos resumos criptográficos dos nodos abaixo. O nodo raiz é chamado de raiz de Merkle.(MERKLE, 1982)

Estas estruturas podem ser utilizadas para realizar uma compactação de diversos resumos criptográficos com o objetivo de deixar mais eficiente a verificação da consistência de um conjunto maior de dados. Para verificar se um resumo criptográfico H faz parte da árvore tendo sua raíz R, é necessário calcular apenas o caminho da árvore em que H supostamente pertence e comparar a raíz calculada RH com R, se $R = RH$ então H pertence a árvore e o conteúdo do arquivo do qual H foi calculado não foi alterado.

3 REVISÃO BIBLIOGRÁFICA

Para melhor compreender o estado da arte acerca da viabilidade de SSI para o meio de diplomas digitais e sua retrocompatibilidade tecnológica, foi realizada uma revisão sistemática da literatura. Como resultado foram selecionados os trabalhos detalhados neste capítulo.

Para a revisão, então, foram criadas três perguntas de pesquisa, a fim de melhor guiar a pesquisa.

- Quais os usos e funcionamentos das tecnologias de Identidade Digital no atual estado da arte?
- Quais as vantagens e desvantagens entre as tecnologias utilizadas para a emissão de diplomas Universitários Digitais?
- O que SSI traz de melhor para os diplomas Universitários Digitais? (Por que SSI?)

Utilizando as perguntas de pesquisa, foram definidas as palavras chaves e sinônimos para a construção da string de pesquisa para a consulta nas bases de dados. Como sinônimos da palavra blockchain, também foram utilizadas as palavras “Hyperledger” e “Hyperledger Indy” por ser uma das tecnologias atuais que trazem o conceito de Identidade Digital em blockchain, e “Bitcoin” e “Ethereum” por serem duas das tecnologias mais conhecidas desenvolvidas sobre a blockchain.

- blockchain: “blockchain” “Hypeledger” “Hyperledger Indy” “Bitcoin” “Ethereum”
- Degree Certificates: “Degree Certificate” “Certificate Degree” “diploma”
- Self- Sovereign Identity:“Self Sovereign Identity” “SSI”

Sendo então construída a string de pesquisa à seguir:

Algoritmo 1 – String de busca utilizada para a revisão sistemática

```
(("blockchain"OR "Hyperledger"OR "Hyperledger Indy"OR "Bitcoin"OR "Ethereum") OR ("Self Sovereign Identity"OR "SSI")) AND ("Degree Certificate"OR "Certificate Degree"OR "diploma")
```

Fonte: O autor.

3.1 RESULTADOS PRELIMINARES DA BUSCA

A Tabela 1 apresenta os dados das bases de dados utilizadas, juntamente com a string de pesquisa e os filtros utilizados para realizar a pesquisa em cada base. Algumas bases possuem restrições do tamanho da string de pesquisa, e portanto, ela foi ajustada para melhor se encaixar nestas restrições.

Ferramenta	String de Pesquisa	Filtros Utilizados
https://scholar.google.com	(("blockchain"OR "Hyperledger"OR "Hyperledger Indy"OR "Bitcoin"OR "Ethereum") OR ("Self Sovereign Identity"OR "SSI")) AND ("Degree Certificate"OR "Certificate Degree"OR "diploma")	Since 2010
https://ieeexplore.ieee.org	(("blockchain"OR "Hyperledger"OR "Hyperledger Indy"OR "Bitcoin"OR "Ethereum") OR ("Self Sovereign Identity"OR "SSI")) AND ("Degree Certificate"OR "Certificate Degree"OR "diploma")	2010-2021
https://dl.acm.org	(("blockchain"OR "Hyperledger"OR "Hyperledger Indy"OR "Bitcoin"OR "Ethereum") OR ("Self Sovereign Identity"OR "SSI")) AND ("Degree Certificate"OR "Certificate Degree"OR "diploma")	Since 2010
https://www.sciencedirect.com	(("blockchain"OR "Hyperledger"OR "Bitcoin"OR "Ethereum") OR ("Self Sovereign Identity"OR "SSI")) AND ("Degree Certificate"OR "Certificate Degree"OR "diploma")	2010-2021; Computer Science; Engineering
https://link.springer.com	(("blockchain"OR "Hyperledger"OR "Hyperledger Indy"OR "Bitcoin"OR "Ethereum") OR ("Self Sovereign Identity"OR "SSI")) AND ("Degree Certificate"OR "Certificate Degree"OR "diploma")	2010-2021, No Preview Content, Computer Science

Tabela 1 – Tabela de Estrutura de busca nas bases de dados.

Os resultados da pesquisa inicial são apresentados na Tabela 2. A tabela se encontra dividida em 5 colunas, trazendo a ferramenta utilizada na primeira coluna. A coluna resultado inicial mostra a contagem não filtrada de resultados que a base de dados enviou como resposta à string de pesquisa. Devido a algumas particularidades dos motores de busca, nem todos puderam utilizar filtros mais finos como área de pesquisa trazendo então uma quantidade maior de trabalhos, visto a quantidade retornada pela ferramenta Google Scholar.

Sendo assim, é necessário aplicar um filtro, para obter então os trabalhos que melhor representam esta pesquisa. As três últimas colunas da Tabela 2 trazem a aplicação de três etapas de seleção dos trabalhos, que funcionam como segue:

- Seleção 1: Nesta etapa foram analisados os títulos dos trabalhos. Os títulos precisam conter pelo menos uma das palavras chave, ou combinação entre elas, estando então dentro do contexto da pesquisa de documentação digital focada em diplomas universitários digitais. Os trabalhos selecionados então passaram para a etapa Seleção 2;

- Seleção 2: Nesta etapa foram analisados os resumos dos trabalhos. Os trabalhos cujos resumos apresentaram relação com as questões de pesquisa ou que traziam solução para os tais seguiram para a Seleção 3;

- Seleção 3: Nesta última etapa, foram então lidos os trabalhos por completo. Os trabalhos que possuem uma proposta que contribui para o tema de pesquisa ou traga uma solução para uma ou mais questões de pesquisa, foram selecionados. Além disso, foi produzido então um texto para cada trabalho selecionado, com foco em: Problema de pesquisa, solução apresentada e comentário crítico sobre a resposta.

Ferramenta	Resultado Inicial	Seleção 1	Seleção 2	Seleção 3
https://scholar.google.com	12500	59	37	27
https://ieeexplore.ieee.org	11	8	5	2
https://dl.acm.org	54	5	3	3
https://www.sciencedirect.com	98	1	0	0
https://link.springer.com	7	0	0	0
Total	12670	73	45	32

Tabela 2 – Tabela dos resultados iniciais da revisão sistemática.

Seguem as referências dos artigos selecionados na Seleção 3. Os trabalhos listados são acompanhados de uma explicação breve, e são agrupados de forma a manter as características em comum próximas.

As maiores preocupações do mercado de trabalho quanto às capacitações de um possível empregado, são relativas à veracidade das alegações feitas em seu currículo. Na atualidade é muito fácil replicar ou forjar um documento que ateste a completude de um curso de ensino superior, para que seja possível obter um emprego com maior facilidade, ou com condições melhores de trabalho. Desta forma, a grande maioria dos trabalhos analisados traz uma forma ou implementação de um sistema cujo objetivo principal é atacar este problema.

Utilizando a tecnologia Blockcerts, (DURANT; TRACHY, 2017) traz a iniciativa do MIT em utilizar a blockchain para o armazenamento e distribuição dos diplomas emitidos, (PETRE; PAQUE; LEJEUNE, 2019) traz o foco para a infraestrutura e os benefícios que a tecnologia traria para a universidade de Louvaine, analisando custos e maneiras de implementação na instituição. (VIDAL; GOUVEIA; SOARES, 2020a) cria uma aplicação baseada em Blockcerts porém agnóstico quanto a tecnologia da blockchain, já que se utiliza de aplicações Web para maior parte de seu funcionamento. (ATAŞEN; ASLAN, 2020) cria um sistema simples na forma de um aplicativo descentralizado, onde transações para os smart contracts deste aplicativo tem como função inserir, recuperar e verificar os documentos. (BUDHIRAJA; RANI, 2019) utiliza a tecnologia Ethereum e propõe um aplicativo descentralizado que utiliza smart contracts para publicar a hash do documento na blockhain e o arquivo em um sistema de arquivos externo. (ČEKE; KUNOSIĆ, 2020) faz uma abordagem genérica quanto ao funcionamento do

sistema, e também utiliza Ethereum e smart contracts para criar um aplicativo descentralizado que armazena os diplomas como novos smart contracts na blockchain.

No trabalho de (KALTYSHEV, 2018) é proposto um sistema baseado em Multichain de armazenamento de documentos na blockchain mais simples onde o documento é armazenado por inteiro na blockchain e pode ser verificado ao se tirar sua hash e consultar a blockchain, ou enviar o documento por completo ao sistema, que fará esta verificação. Estes trabalhos se afastam do conceito de SSI pois parte da emissão ou da verificação da credencial exigem o compartilhamento completo do documento.

(ABREU; COUTINHO; BEZERRA, 2020) utiliza Ethereum para trazer uma prova de conceito de uma arquitetura que utiliza a blockchain como meio de emissão e verificação de diplomas. A arquitetura prevê o uso de aplicativos gráficos para o acesso ao sistema e API's para comunicação entre as partes, além de bancos de dados externos para armazenamento dos documentos. (BHUMICHITR; CHANNARUKUL, 2020) traz um aplicativo descentralizado que utiliza smart contracts para armazenar o histórico do aluno na forma de hashes das disciplinas cursadas, e em sua conclusão do curso emitir e armazenar seu diploma automaticamente.

(LEKA; SELIMI, 2020) foca na parte de autenticação ao sistema, trazendo a proposta de um sistema com a tecnologia Ethereum utilizando smart contracts para garantir a autenticação e autorização dos usuários ao acessarem a blockchain privativa. (BRUNNER; KNIRSCH; ENGEL, 2019) propõe um sistema onde a emissão de um documento digital se dá por uma transação na blockchain contendo a hash do documento, e os documentos em si se mantém em posse de seus donos. A verificação se dá ao se tirar a hash do documento original e compará-la com a da transação existente na blockchain pública.

(MORISIO; ARDITO; YOKUBOV, 2018) implementa um sistema de graduação utilizando Ethereum e Smart Contracts, onde as notas dadas aos alunos são representadas por transações onde tokens marcados são enviados como transações na Blockchain. Cada tipo de token representa sua disciplina, e o histórico do aluno então fica salvo na blockchain, sendo facilmente verificável. (ARENAS; FERNANDEZ, 2018), utilizando a tecnologia Multichain, também trás a publicação dos documentos na forma de transações na blockchain, onde o aluno pode realizar consultas para obter o seu documento.

(YEH, 2018) cria um sistema robusto baseado em Ethereum para a emissão e validação dos documentos emitidos, além de criar um sistema de verificação que divide o arquivo em duas partes armazenadas em locais diferentes para serem juntas quando for necessária a verificação das informações. (DIMA et al., 2018) propõe um sistema baseado na tecnologia Multichain e utilizando APIs web escritas em Python utilizando a biblioteca Flask. O sistema proposto possui três tipos de nodos, autoridade, instituição e aluno, onde a autoridade permite a entrada de novas instituições na rede, a instituição pode emitir os documentos e o aluno pode recebê-los e verificá-los. A emissão de um documento se dá por uma transação monetária a um endereço compartilhado pela autoridade e pela instituição contendo a hash do documento e os endereços na blockchain da instituição e do aluno, e a revogação é dada ao se "gastar" este recurso enviado.

De maneira semelhante, (AVERIN; SNEGIREVA; LADEJSHCHIKOV, 2020) não es-

pecifica a tecnologia mas propõe um sistema baseado em blockchain onde existem dois papéis específicos, Emissores e Receptores. Neste sistema, a instituição e o aluno possuem seus endereços próprios na blockchain onde a emissão do diploma e a avaliação de cada disciplina e dada na forma de uma transação endereçada ao aluno. A verificação então consiste em buscar todas as transações no sistema que possuam como destinatário o aluno, a fim de validar a autenticidade do documento. (GHAZALI; SALEH, 2018) também trás uma proposta de um sistema onde o registro da emissão dos documentos é dado pelo envio de transação contendo a hash do documento na blockchain. Neste modelo, as transações são assinadas pela instituição emissora o que também garante a procedência do documento.

(LIU; GUO, 2019) propõe um sistema complexo utilizando Hyperledger Fabric com smart contracts nomeados Foreground System (API ou Webservice), Endorser, Orderer e Commiter. Este sistema também se utiliza de programas terceiros de compartilhamento de mensagens, e tem como foco a escalabilidade e segurança contra falhas do sistema em si. (SCHÄR; MÖSLI, 2019) propõe um sistema conceitual sem especificar a tecnologia, onde a emissão de um documento consiste em emitir uma transação com a hash de um documento em formato pdf para um smart contract que a criptografa e a armazena em seu armazenamento. A verificação consiste em tirar a hash do documento novamente e compará-la com a hash descriptografada recebida do smart contract. (HAN, 2018) foca no compartilhamento do documento e apresenta um projeto conceitual onde os papéis dos nodos do sistema são divididos em provedor, este que pode publicar os diplomas, indivíduo que pode somente realizar verificações e mineradores, que validam as transações.

(BAHRAMI; MOVAHEDIAN; DELDARI, 2020), traz um sistema baseado na tecnologia Hyperledger Fabric, que se utiliza de Smart Contracts juntamente com diferentes papéis entre os usuários para o seu correto funcionamento. (PALMA et al., 2020) utiliza a tecnologia Ethereum e smart contracts para criar o sistema e cita três papéis principais para os usuários do sistema, RA (Autoridade Reguladora), HEI (Instituição de Ensino Superior) e Student (Aluno), além dos smart contracts nomeados Curriculum (Currículo) e Authority (Autoridade). (NGUYEN et al., 2018) também usa Ethereum e segue neste mesmo princípio com quatro tipos de smart contracts, Ownable (Pertencível), Student (Aluno), Issuer (Emissor) e System (Sistema). (SAYED, 2019) utiliza Ethereum e traz os smart contracts nomeados de Course (Disciplina), Degree Program (Curso), Student (Aluno) e Identity Management (Administração de Identidade). Estes trabalhos se assemelham por criar aplicativos descentralizados utilizando smart contracts, e papéis específicos para cada entidade pertencente ao sistema, ou para os smart contracts em si, onde o funcionamento do sistema se dá pelas relações entre estes papéis. De maneira genérica, há um papel que possui autoridade de emissão, e um papel para o estudante. Outros papéis podem ser adicionados que contribuem para o funcionamento dos sistemas, como a Autoridade Reguladora de (PALMA et al., 2020) ou o System de (NGUYEN et al., 2018), que possuem maior autoridade e podem realizar ações sobre os outros papéis.

(PATEL, 2020) sugere a idéia de utilizar árvores de Merkle para a emissão em lotes dos diplomas. Neste contexto apenas a raíz da árvore de diplomas é publicada, e os caminhos

de verificação da árvore são publicados em um sistema de arquivos IPFS. Seguindo esta idéia, (SAN; CHOTIKAKAMTHORN; SATHITWIRIYAWONG, 2019) também propõe um sistema que utiliza árvores de Merkle, onde cada folha da árvore é constituída pela hash do histórico de aluno e de seu documento. Neste modelo, o aluno fica em posse de sua hash, sendo possível realizar a verificação da autenticidade do documento através da árvore.

Se afastando dos sistemas de criação e compartilhamento de credenciais, (VIDAL; GOUVEIA; SOARES, 2020b) foca no aspecto da revogação dos documentos emitidos, onde a emissão do documento é dada por uma transação na blockchain e sua revogação pelo "gasto" do valor recebido na transação, facilitando o processo para verificar e revogar a credencial.

(LIU, 2020) reune três sistemas existentes que implementam identidades digitais, Sovrin, uPort, e Shocard, além de trazer seus funcionamentos e compará-los com as leis da identidade. São mostradas as características principais de cada um e analisadas as capacidades dos sistemas propostos, incluindo suas capacidades de segurança e privacidade, trazendo como tema também Self-sovereign Identity. Este trabalho é bastante completo, trazendo descrições elaboradas e tabelas comparativas complexas, o que auxiliam ao leitor se inteirar do estado da arte da tecnologia, e conhecer os trabalhos realizados até então. Dessa forma, é possível dirigir uma pesquisa a um tema específico, graças a esta comparação feita.

(CASTRO; AU-YONG-OLIVEIRA, 2021) realiza uma revisão da literatura a fim de trazer o estado da arte dos trabalhos enviados na plataforma Scopus, que tenham como temas blockchain e diplomas de Ensino Superior. Os resultados mostram que diversas das pesquisas encontradas são feitas de forma localizada, tendo como foco as necessidades da localidade em que são efetuadas, além de trazer um ponto bastante importante e pouco abordado, que é a mobilidade dos possuidores dos documentos digitais. Os autores chegam a conclusão que a blockchain é uma evolução para os diplomas digitais, trazendo soluções para os problemas mais comuns como fraude, mobilidade e dificuldade de autenticar os documentos.

Em (LEPIANE et al., 2019) os autores trazem uma análise completa de como é o cenário brasileiro de emissão do diploma, trazendo as leis relacionadas, e os problemas identificados quanto ao método de emissão, armazenamento e verificação de diplomas nas instituições de ensino Brasileiras. O modelo conceitual criado utiliza o sistema de chaves públicas da ICP-Brasil para criar e assinar diplomas digitais, que tem seu formato especificado por arquivos de "schema". Também são tratados os problemas referentes aos certificados digitais atrelados às assinaturas dos documentos. Esses diplomas em formato XML, seriam emitidos e assinados pela instituição, e armazenados em um sistema de arquivos governamental ou o sistema digital da própria universidade, e seriam também criadas imagens dos diplomas com códigos QR e URL's que apontam para o arquivo nos sistemas da instituição e para Listas de Revogação, a fim de verificar o documento.

(ASIRI, 2020) traz uma pesquisa demográfica bastante aprofundada do conhecimento e aceitação de sistemas de armazenamento e distribuição de diplomas de ensino superior em formatos digitais e em blockchains. Embora não traga implementação ou desenvolvimento dos sistemas em si, este estudo mostra que vários dos problemas sendo trabalhados são reais e

que afetam boa parte do público, além de trazer resultados quanto aos níveis de conhecimento da população e níveis de aceitação o que podem dar uma ideia das dificuldades que seriam enfrentadas ao se implementar um sistema deste tipo em um cenário real.

3.2 ANÁLISE DA REVISÃO

Diversos autores utilizam as tecnologias de blockchain para o armazenamento dos diplomas Digitais, o que garante temporalidade e imutabilidade as informações (CASTRO; AUYONG-OLIVEIRA, 2021). Dependendo do grau de privacidade necessário em cada implementação, a blockchain é utilizada para armazenar o documento completo, ou apenas um resumo criptográfico do mesmo, que é então armazenado em um sistema externo, como por exemplo o IPFS (InterPlanetary File System)(PROTOCOL LABS, 2020). Na Tabela 3 são apresentados os trabalhos correlatos encontrados no processo de revisão, classificados de acordo com os seguintes critérios:

- **Tecnologia Utilizada** - *Qual a tecnologia blockchain utilizada para a construção da solução?*
- **Utilização de smart contracts** - *A solução proposta pode utilizar smart contracts para auxiliar o funcionamento ou depende completamente deles no caso de Aplicativos Descentralizados.*
- **Propriedades de SSI** - *O sistema se adéqua completamente ou parcialmente aos critérios de SSI?*
- **Retrocompatibilidade** - *O trabalho aborda ou fala sobre a possibilidade de integrar documentos gerados de outras formas legadas?*

Na tabela, o símbolo ✓ demonstra uma entrada positiva, o símbolo ✔✗ demonstra entradas parciais, e o símbolo ✗ demonstra entradas negativas.

Trabalho	Tecnologia	Smart Contracts	SSI	Aborda Retrocompatibilidade
(PETRE; PAQUE; LEJEUNE, 2019)	Blockcerts	✓	✔✗	✗
(BAHRAMI; MOVAHEDIAN; DELDARI, 2020)	Hyperledger Fabric	✓	✗	✗
(MORISIO; ARDITO; YOKUBOV, 2018)	Ethereum, ERC20 Tokens	✓	✗	✗
(DURANT; TRACHY, 2017)	Blockcerts	✓	✔✗	✗
(LIU, 2020)	Sovrin, uPort, Shocard	✓	✔✗	✗

Cont. Tabela 3				
Trabalho	Tecnologia	Smart Contracts	SSI	Aborda Retrocom-patibilidade
(KALTYSHEV, 2018)	Multichain	✗	✗	✗
(LEKA; SELIMI, 2020)	Ethereum	✓	✗	✗
(HAN, 2018)	Undisclosed	✓	✗	✗
(ABREU; COUTINHO; BEZERRA, 2020)	Ethereum	✓	✗	✗
(GHAZALI; SALEH, 2018)	Não Especificado	✗	✗	✗
(VIDAL; GOUVEIA; SOARES, 2020b)	Não Especificado	✗	✗	✗
(PATEL, 2020)	Ethereum	✓	✗	✗
(BRUNNER; KNIRSCH; ENGEL, 2019)	Não Especificado	✗	✗	✗
(YEH, 2018)	Ethereum	✓	✗	✗
(PALMA et al., 2020)	Ethereum	✓	✗	✗
(ATAŞEN; ASLAN, 2020)	Ethereum	✓	✗	✗
(BUDHIRAJA; RANI, 2019)	Ethereum	✓	✗	✗
(CHENG, 2020)	Hyperledger Fabric	✓	✗	✗
(DIMA et al., 2018)	Multichain	✗	✗	✗
(LIU; GUO, 2019)	Hyperledger Fabric	✗	✗	✗
(AVERIN; SNEGIREVA; LADEJSHCHI-KOV, 2020)	Não Especificado	✗	✗	✗
(ARENAS; FERNANDEZ, 2018)	Multichain	✗	✗	✗
(VIDAL; GOUVEIA; SOARES, 2020a)	Blockcerts, Bitcoin, Ethereum	✗	✗	✗
(SCHÄR; MÖSLI, 2019)	Ethereum	✓	✗	✗
(SAYED, 2019)	Ethereum	✓	✗	✗
(BHUMICHITR; CHANNARUKUL, 2020)	Hyperledger Fabric	✗	✗	✗
(NGUYEN et al., 2018)	Ethereum	✓	✗	✗
(SAN; CHOTIKAKAMTHORN; SATHITWIRIYAWONG, 2019)	Não Especificado	✗	✗	✗
(ČEKE; KUNOSIĆ, 2020)	Ethereum	✓	✗	✗
Nosso	Hyperledger Indy	✗	✓	✓

Tabela 3 – Tabela de Trabalhos Correlatos.

Na Tabela 3 não foram incluídos três trabalhos, por não se encaixarem nos critérios de comparação. (ASIRI, 2020) realiza um estudo demográfico sobre a aceitação dos sistemas de documentação digital em blockchain, mas que é de grande relevância conceitual para a pesquisa apresentada. (CASTRO; AU-YONG-OLIVEIRA, 2021) faz uma revisão sistemática apenas na plataforma Scopus, e mostra que as pesquisas encontradas focam muito nas realidades locais dos pesquisadores, trazendo então alguns pontos importantes para o estudo deste tópico como

a portabilidade. Por fim, (LEPIANE et al., 2019) não utiliza a blockchain, mas propõe uma solução que se aproxima daquela proposta pelo Ministério da Educação (MINISTÉRIO DA EDUCAÇÃO BRASILEIRO, 2018), ao utilizar a ICP-Brasil, arquivos XML e sistemas de arquivos distribuídos para o armazenamento.

Para além da classificação, uma análise dos trabalhos apresentados na Tabela 3 mostra que o interesse pelo armazenamento de diplomas em blockchain vem aumentando ao longo do tempo, com um trabalho publicado em 2017, oito em 2018, oito em 2019, e quatorze trabalhos em 2020.

Inclusive a própria tecnologia blockchain vem ganhando mais destaque o que pode indicar as escolhas de tecnologia dos artigos encontrados, pois doze usam Ethereum, quatro Hyperledger Fabric, três Multichain, três Blockcerts, e apenas um utiliza o próprio Bitcoin, o que pode ser atribuído as datas de publicação das tecnologias.

Por último, é importante notar que poucos são os trabalhos encontrados que possuem características de SSI. Isto pode ser constatado, pois as informações não estão em total controle do usuário, ou mais informação do que é necessária é discorrida. Alguns dos trabalhos, por exemplo, armazenam o documento completo na blockchain, outros passam o documento por uma função de resumo criptográfico, armazenando apenas a hash na blockchain. Estes dois exemplos tornam o documento publicamente verificável, porém exigem que o documento original seja exposto, a fim de realizar essa verificação.

Este trabalho trás como contribuição principal o desenvolvimento na prática de um protocolo e um protótipo que se aproximem ao máximo dos casos de uso reais deste tipo de sistema e que possuam retrocompatibilidade com documentos emitidos em outros sistemas legados ou até em papel, levando em conta a Legislação Brasileira e a LGPD, além de trazer discussões sobre como este protocolo poderia ser implementado na prática.

3.3 ANÁLISE DOS RESULTADOS

Ao se analisar os dados coletados de todos os trabalhos, é notável que a preocupação com a segurança e a verificação dos diplomas digitais vai aumentando conforme a tecnologia vai amadurecendo com 1 artigo em 2017, 8 em 2018, 9 em 2019 e 15 em 2020, e acordo com os artigos selecionados após a etapa da seleção 3 desta pesquisa. Não só isso, como temos algumas respostas para as perguntas de pesquisa, delineadas no início deste trabalho.

3.3.1 Quais os usos e funcionamentos das tecnologias de Identidade Digital no atual estado da arte?

A grande maioria dos trabalhos encontrados trazem implementações e soluções para os diplomas digitais, analisando problemas em comum quanto à emissão, armazenamento e verificação dos documentos em sua forma digital. Estes problemas são muito bem descritos

em (SAYED, 2019), que evidencia vários tipos de fraudes e esquemas que podem resultar em documentos falsificados, ilegítimos, ou verdadeiros, porém obtidos de forma ilegítima.

Estas soluções analisam estes problemas, e trazem propostas e implementações de sistemas que se utilizam de variadas tecnologias blockchain existentes, mostrando como cada problema seria solucionado pelo uso desta tecnologia.

Dentre os trabalhos selecionados, 4 utilizam Hyperledger Fabric como tecnologia principal, 12 utilizam Ethereum, 1 utiliza Bitcoin, 3 utilizam Blockcerts, 3 utilizam Multichain, 2 trazem propostas genéricas, para qualquer blockchain, e dentre todos, 15 utilizam smart contracts para construir seus sistemas, e 2 complementam suas propostas com sistemas terceiros de mensagens e cadastro.

3.3.2 Quais as vantagens e desvantagens entre as tecnologias utilizadas para a emissão de diplomas Universitários Digitais?

Todos os trabalhos que trazem uma implementação, proposta, ou modelo analisam a eficiência do sistema apresentado e o comparam com o sistema utilizado hoje em dia, de armazenamento e emissão dos diplomas em papel moeda. As vantagens encontradas, se comparadas com este sistema variam, dependendo da implementação.

Alguns trabalhos como o de (MORISIO; ARDITO; YOKUBOV, 2018), focam em criar um sistema que seja rápido e prático para a submissão do histórico do aluno, outros como (PALMA et al., 2020),(BUDHIRAJA; RANI, 2019), e (BHUMICHITR; CHANNARUKUL, 2020), trazem implementações de um sistema completo, se preocupando em atacar as vulnerabilidades existentes nos sistemas de papel.

Estes problemas se resumem a fraudes e forjas, onde o documento é copiado ou obtido de maneira ilegítima. Nesses casos, a verificação da autenticidade é demorada ou impossível. Uma das razões é o envio do documento, que normalmente ocorre com uma cópia em folha comum do documento ou foto digital, o que deixa os mecanismos anti fraude do papel moeda inúteis e força a verificação a ser feita contatando a instituição. Este contato pode demorar dias ou semanas para retornar o resultado, e caso a instituição tenha falido ou desaparecido a verificação se torna impossível.

As vantagens então dos sistemas que se utilizam de blockchain ficam claras, analisando os problemas citados. blockchain por ser um sistema distribuído, não possui apenas um ponto de falha, além de trazer registros ordenados pela data de envio, com timestamps, o que aumenta a quantidade de informação possível de ser resgatada e verificada. Depois de um certo número de transações, os registros são considerados imutáveis, além de serem publicamente verificáveis em blockchain públicas.

Outra vertente são blockchains privadas, que, mesmo perdendo certo poder nos quesitos “Sistema Distribuído” e “Volume de transações”, ganha vantagens nos seguintes quesitos:

- Custo - as transações não precisam de incentivos monetários para serem aceleradas e

processadas.

- Autenticação - blockchains privadas possuem “Papéis” ou funções delegadas a certos endereços.
- Customização - os algoritmos de consenso e canais de mensagem podem ser customizados, para que o sistema fique mais seguro contra transações não validadas.

Outra vantagem é a automatização, com smart contracts. Como mostrado em (NGUYEN et al., 2018), (VIDAL; GOUVEIA; SOARES, 2020a), e (ATAŞEN; ASLAN, 2020), é possível utilizar smart contracts em blockchains que os suportem, para que os sistemas de coleção de dados e emissão de documentos sejam completamente automatizados. Não só isso, smart contracts permitem que os aplicativos sejam executados dentro da blockchain, de forma descentralizada, diminuindo a complexidade de aplicativos externos para a lógica do sistema.

3.3.3 O que SSI traz de melhor para os diplomas Universitários Digitais? (Por que SSI?)

O principal objetivo de SSI é trazer a responsabilidade sobre a privacidade de um usuário para ele próprio. Nenhuma outra organização ou indivíduo seria responsável pelos dados de um indivíduo a não ser ele próprio, sendo assim, o indivíduo que escolheria com quem e quanta informação compartilhar a qualquer momento.

Alguns trabalhos como (YEH, 2018), demonstram o funcionamento do sistema de forma que se aproxime do conceito de SSI. Ou seja, as credenciais estão em posse do aluno, e ele quem decide compartilhar suas credenciais. Não só isso, como o processo de verificação não expõe dados do aluno, no caso da verificação por QR Code do trabalho acima citado.

SSI traz ao indivíduo a sua identidade, e a responsabilidade de mantê-la. Isso por si só é uma vantagem, já que assim, o indivíduo tem total controle sobre seus dados pessoais, com quem compartilhá-los e como.

López (LóPEZ, 2020) enumera alguns dos benefícios que SSI traz para a documentação digital, como Interoperabilidade, Pseudonimidade, Pertencibilidade, Portabilidade, Recuperação, Escalabilidade e Segurança. SSI também possui diversas vantagens pelo seu funcionamento intrínseco com blockchain, possuindo então as mesmas vantagens de descentralização e escalabilidade.

Para os diplomas digitais, SSI permitiria que o aluno obtivesse seu diploma diretamente da Instituição, com uma cerimônia de emissão mais rápida e segura, onde uma troca de transações adicionaria o diploma a sua carteira. Este diploma existiria somente na carteira pessoal do aluno, e, poderia ser facilmente verificado por possíveis empregadores, com sistemas de prova de conhecimento zero, ou até provas abertas, de forma rápida, e fácil, mesmo que a instituição venha a sumir devido a falência.

SSI também garante o direito de ser esquecido. Provas enviadas pelo aluno somente possuem utilidade se executadas por quem as requisitou, e caso sejam provas de conhecimento

zero, as informações do aluno portanto não seriam de conhecimento do empregador, e não poderiam ser adicionadas a listas de e-mails ou vendidas.

3.3.4 Conclusões sobre a Revisão

Tendo realizado esta pesquisa, pode-se concluir que o interesse em armazenamento digital e verificação de documentos digitais está crescendo, assim como o interesse na privacidade, e segurança do usuário também. Este é um tema que está sendo pesquisado ao redor do mundo, e também pode se perceber que SSI seria um passo lógico para o aprimoramento da segurança e privacidade do usuário, no contexto da documentação digital.

Os trabalhos encontrados nessa pesquisa também trazem pontos de discussão sobre a documentação digital, estes pontos são importantes de serem analisados em uma possível implementação desta tecnologia como a revogação das credenciais, e possíveis formas de emissão e armazenamento dos documentos na blockchain.

4 PROPOSTA: PROTOCOLO DE DIPLOMA DIGITAL AUTO-SOBERANO COM RETROCOMPATIBILIDADE TECNOLÓGICA

Como objetivo principal deste trabalho, será proposto um protocolo para emissão de créditos e diplomas de ensino superior de forma auto-soberana com retrocompatibilidade tecnológica. Seu maior objetivo é poder ser analisado quanto a sua viabilidade e segurança, para servir como base ou inspiração para uma possível implementação real no Brasil.

O protocolo proposto neste capítulo é baseado nas características do funcionamento do Hyperledger Indy. Primeiro, apresenta-se as definições sintáticas dos elementos utilizados na narração (§4.1). Logo após apresentamos as premissas e entidades do protocolo (§4.2). Na sequência apresentamos os objetos e seus tipos (§4.3) e por fim apresentamos protocolo e sua narrativa (§4.4).

4.1 DEFINIÇÕES SINTÁTICAS

A fim de garantir ao leitor compreensão clara da notação utilizada para descrever o protocolo, na sequência apresentamos os elementos sintáticos utilizados para descrever o nosso protocolo:

Mensagem Comum - Representa uma mensagem utilizada para enviar informações entre as partes envolvidas. Uma mensagem comum do protocolo poder ser vista após no listing 4.1. Neste tipo de comunicação, o **emissor** envia a mensagem para um **receptor**, que podem ser usuários comuns ou instituições. A mensagem possui um **conteúdo**, por exemplo uma oferta de credencial. Algumas mensagens exigem que certos **requisitos** sejam atendidos para que possam ser enviadas. Os **requisitos** são exigidos de usuários ditos **possuidores**. Por fim, a mensagem pode ter um conteúdo composto de mais de uma **informação**.

<Emissor> → <[Possuidor(Requisitos)] Conteúdo (Informação Incluída)> → <Receptor>

(4.1)

Condicional - Representa uma divisão do caminho de execução do protocolo, como as condicionais das linguagens de programação usuais, através da avaliação da expressão após a *tag* **IF**. Se for avaliada como verdadeira, é executado o fluxo após a *tag* **DO**. Senão, continua-se a execução a partir da *tag* **FI**. Um exemplo pode ser visto no Listing 4.2.

IF: <Expressão> DO: <Fluxo A > FI:

(4.2)

4.2 PREMISSAS E ENTIDADES

A fim de podermos discutir na sequência a aplicabilidade e a corretude da nossa proposta enquanto solução, é importante apresentarmos as premissas tomadas para a construção do protocolo, e a descrição clara e objetiva das entidades nele envolvidas:

Premissas - Assume-se que a requisição de prova (Proof Request) traga como requisitos todas as informações necessárias e cabíveis para um dado contexto. Por exemplo, a prova de um diploma para uma aplicação de emprego pode exigir o nível do diploma (e.g., Graduação, Mestrado e Doutorado), a Instituição de Ensino Superior (IES ou HEI), a média final, o curso e o ano de formatura.

Entidades - As entidades que operam o protocolo são apresentadas na Tabela 4 e levam em consideração os vários atores que se apresentam em nosso protocolo.

Entidade	Descrição
HEI	Instituição de Ensino Superior - Emite as credenciais de diploma e Disciplina;
RA	Autoridade Reguladora - Dá à HEI a credencial de HEI, que permite a HEI emitir as credenciais;
S	Estudante - Estudante que cursa as disciplinas e recebe então as credenciais da HEI;
L	Ledger (Hyperledger Indy) - Ledger onde são publicadas os Schemas, Definitions e Verinyms;
V	Verificador - Indivíduo que requisita uma prova e a executa, a fim de obter confirmação de uma afirmação.

Tabela 4 – Entidades participantes do protocolo.

A relação entre estas entidades é demonstrada na figura 3.

4.3 DESCRIÇÃO DOS OBJETOS

Neste subcapítulo apresentamos a definição dos tipos de objetos e na sequência os objetos utilizados no protocolo. Os tipo de dados de objetos são dados pela plataforma e os objetos são a instanciação destes tipos de acordo com as necessidade do protocolo. Eles são apresentados na sequência:

Definição dos Tipos de Objetos - Os objetos utilizados no protocolo são baseados naqueles utilizados pelo Hyperledger Indy e são apresentados na Tabela 5.

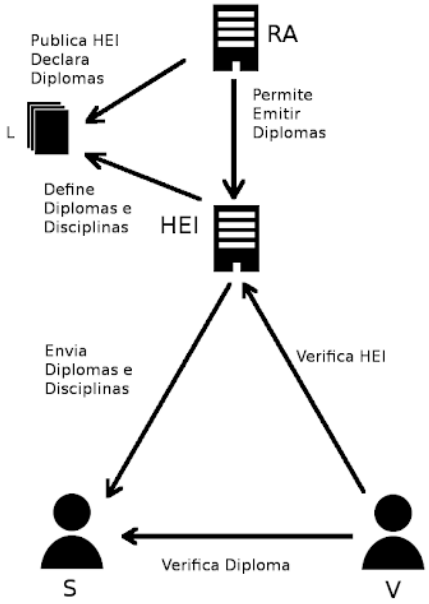

Figura 3 – Demonstração da relação entre as entidades do protocolo.
fonte: autor.

Objeto	Descrição
DID	Decentralized Identifier, é uma sequência de caracteres que identifica um usuário da rede, este que pode ser uma instituição ou uma pessoa. Um DID deve se referir a apenas um usuário, porém um usuário pode ter mais de um DID. Até ser publicado na Ledger, um DID é um pseudônimo (pseudonym). Quando publicado na Ledger, um DID se torna um ID público (verynim), e é atrelado então a uma identidade pública, como uma instituição. Apenas indivíduos com IDs públicos podem criar e emitir credenciais.
Credential Schema	É um esqueleto de uma credencial, onde são definidos o nome, versão e atributos que a credencial irá conter. Este esqueleto deve ser publicado na Ledger antes de se criar uma Credential Definition.
Credential Definition	É a definição da credencial, baseada no schema, ela define as configurações de uma credencial, como suporte a revogações, seu tipo e caso seja revogável o repositório onde buscar esta informação. Deve ser enviada para a Ledger para que seja criada uma Credential.
Credential	É a credencial em si. É baseada na Schema e na Definição, e contém as informações do portador. É guardada na carteira do usuário e pode ser utilizada para criar Provas (Proofs) que podem ser enviadas para outros usuários e avaliadas, sobre os dados existentes na credencial, de forma que as informações não sejam legíveis, nem armazenáveis.
Proof	Pode ser criada a partir de uma Credential, e opcionalmente por uma Proof Request. Ela contém a lógica necessária para se provar uma ou mais afirmações acerca de um usuário, de forma que essa informação não seja conhecida nem armazenada por quem deseja realizar a prova.
Proof Request	Requisição criada a partir de uma Credential Schema e Credential Definition. Enviada a um usuário que então a utiliza para criar a prova (Proof), que seria retornada para o requisitante.

Cont. Tabela 5	
Objeto	Descrição
Verynim	Mensagem que cadastra na Ledger o DID de uma instituição ou identidade pública.

Tabela 5 – Objetos utilizados no protocolo.

Objetos - Dentro do protocolo criamos alguns objetos próprios baseados nos tipos acima. Abreviações e descrições destes objetos utilizados no protocolo são apresentado na Tabela 6.

Entidade	Descrição
DIP	Credencial de diploma - O diploma em si;
CCD	Credencial de Conclusão de Disciplina - Opcional, depende da implementação, uma HEI pode acumular credenciais de disciplina do aluno e exigi-las na hora de emitir um diploma;
CED	Credencial de Permissão de Emissão de diploma - Credencial que a RA dá à HEI para permiti-la a emitir Credenciais de diplomas.

Tabela 6 – Objetos utilizados no protocolo.

4.4 PROTOCOLO

Com base nos trabalhos analisados e levando em consideração as definições já dadas neste capítulo, queremos propor um protocolo (Algoritmo 2) para emissão de créditos e diplomas de ensino superior de forma auto-soberana. Este protocolo, além de permitir grandes avanços na atual iniciativa do diploma Digital desencadeada pelo Ministério da Educação do Brasil, também possui mecanismos que permitem retrocompatibilidade tecnológica, o que permite uma migração gradual e um salto tecnológico a partir de vários pontos de partida.

Na apresentação do protocolo, conforme o Algoritmo 2, pode-se identificar no primeiro passo (linhas 1 e 2) a autoridade Reguladora (RA) publica na Ledger a definição da Credencial de Permissão de Emissão de diploma (CED). Isto permite que a RA emita estas credenciais e as distribua dando a permissão para Instituições de Ensino Superior (HEI) de emitir diplomas, e também permite revogá-las. Na linha 4 a RA define o Schema da credencial do diploma, o que permite que na linha 6, as HEIs o definam e possam emitir seus próprios diplomas.

Nas linhas 8 a 10, através de canais privados de comunicação, a RA oferece então a credencial de CED para a HEI, e na linha 12, publica o verynim da HEI. Isto mostra que a RA confia que o DID publicado é de fato o DID oficial da HEI.

De forma opcional, é possível realizar o armazenamento do histórico escolar do aluno S, conforme ele progride no meio acadêmico. Para isso, nas linhas 14 e 15, a HEI cria o schema

Algoritmo 2 – Protocolo completo de emissão de diploma digital, desde a permissão dada pela RA até o recebimento do diploma pelo aluno e subsequente prova requisitada por um empregador

```
1.  RA → CED Schema → L
2.  RA → [CED Schema] CED Definition → L
3.
4.  RA → DIP Schema → L
5.
6.  HEI → [DIP Schema] DIP Definition → L
7.
8.  RA → CED Cred Offer (CED Schema, CED Definition) → HEI
9.  HEI → [CED Cred Offer] CED Cred Request → RA
10. RA → [CED Cred Request] CED (Dados HEI) → HEI
11.
12. RA → Verynim (HEI) → L
13.
14. HEI → CCD Schema → L
15. HEI → CCD Definition → L
16.
17. HEI → CCD Cred Offer (CCD Schema, CC Def) → S
18. S → [CCD Cred Offer] CCD Cred Request →HEI
19. HEI → [CCD Cred Request] CCD → S
20.
21. HEI → [S(CCD)]Proof Request → S
22. S → [Proof Request] Proof (CC) → HEI
23. HEI → Verify Proof → HEI
24.
25. IF: Verify Proof
26. DO:
27. HEI → DIP Cred Offer (DIP Schema, DIP Def) → S
28. S → [DIP Cred Offer] DIP Cred Request →HEI
29. HEI → [DIP Cred Request] DP → S
30. FI:
31.
32. V → [DIP]Proof Request → S
33. S → [Proof Request] Proof (DIP) → V
34. V → Verify Proof → V
35.
36. V → [CD]Proof Request → HEI
37. HEI → [Proof Request] Proof (CD) → V
38. V → Verify Proof → V
```

Fonte: O autor.

e a definição de uma Credencial de Conclusão de Disciplina (CCD). Ao final de um semestre, para cada disciplina que o aluno completar com sucesso, nas linhas 17 a 19, a HEI oferece uma CCD referente à disciplina concluída ao aluno, via canais privados. O conjunto de credenciais de disciplinas concluídas que o aluno acumula se torna o histórico escolar.

Após completar todas as disciplinas necessárias o aluno se qualifica para receber o diploma. Primeiramente a HEI exige que o aluno possa provar que todas as disciplinas necessárias foram concluídas. Para isso, na linha 21, a HEI envia uma Proof Request com todos os requisitos para o aluno por meios de canais privados. O aluno utiliza esta Proof Request, juntamente com as CCDs em sua posse para gerar uma prova (Proof) que satisfaça as requisições e a envia de volta para a HEI, também por canais privados, na linha 22. Caso falte alguma CCD, o aluno não conseguirá responder a exigência. Por fim, na linha 23 a HEI realiza a verificação da prova.

Este processo possui mais etapas externas, como verificações de documentos e assinaturas de administradores e diretores da HEI, além de contemplar a legislação para a emissão. A assinatura digital da ICP-Brasil também pode fazer parte do documento, já que a legislação brasileira a reconhece como oficial.

Seguindo por este caminho, caso a prova seja verificada com sucesso na linha 25, nas linhas 27 a 29 a HEI então oferece ao aluno a credencial de diploma, por meio de canais privados. O armazenamento do histórico e consequente verificação não são obrigatórios para o protocolo. A verificação do histórico, ou diploma pré-existente pode ser realizada por meios externos, culminando apenas no envio da credencial do diploma, caso a verificação externa tenha êxito.

Em um ambiente profissional, como uma aplicação de emprego, o aluno será requisitado a mostrar uma prova de que possui um diploma de ensino superior para ser considerado como futuro empregado. Nas linhas 32 a 34, o empregador/verificador (V) envia a Proof Request para o aluno, que a responde com a credencial de seu diploma, por canais privados. Ao receber a credencial o empregador pode verificar a credencial. Opcionalmente o empregador pode querer verificar a validade da instituição em si, e realiza o mesmo procedimento, ao enviar a Proof Request para a HEI, receber a prova com a CED e a verificar nas linhas 36 a 38.

Neste modelo ainda é possível provar utilizando um prova de conhecimento zero que o aluno tem uma competência específica em um determinado grau, apresentando-se por exemplo a uma prova de um determinado valor de nota em algum CCD que ele tenha relacionado a uma credencial DIP. Ainda é importante frisar que este modelo facilmente comporta a tradução de históricos e diplomas anteriores mesmo que emitidos em papel, desde que exista uma entidade que faça as asserções neste sistema. Uma modificação simples seria a criação de entidades Notariais, as quais poderia ter acreditação por parte da RA para fazer asserções sobre diplomas que já foram emitidos anteriormente.

O protocolo gerado cobre os casos de criação ou emissão de um diploma digital no ensino superior, que pode ou não levar em conta o histórico escolar do aluno, conforme ele progride no caminho acadêmico. Por sua flexibilidade, a conversão de documentos é uma so-

lução agnóstica em relação à tecnologia, ou seja, não depende de onde o documento tenha sido emitido anteriormente, seja em papel, via digital por arquivo XML (MINISTÉRIO DA EDUCAÇÃO BRASILEIRO, 2018), ou em uma blockchain pública (PALMA et al., 2020), é possível a conversão ou criação deste documento no formato SSI. A origem do documento só determina o grau de automação que se pode ter neste processo.

Este protocolo exige que todos os integrantes de seu funcionamento façam parte do sistema que o implementaria. Para gerar, receber e verificar os diplomas, é necessário que a instituição, o aluno e o verificador estejam conectados ou usem o sistema. Uma conexão a internet também é necessária para as trocas de mensagens, e mesmo que sejam privados podem criar vulnerabilidades.

5 PROTÓTIPO E MODELO

Como forma de realizar testes práticos, e aferir a viabilidade do protocolo proposto, um protótipo mínimo foi desenvolvido.

O protótipo desenvolvido foi implementado em um formato que permita a completa execução do protocolo, porém, em um estado bastante simplificado, contendo apenas o essencial para que fosse possível evidenciar a sua viabilidade. Para simplificar o desenvolvimento, o RA tem o poder de publicar seus próprios DIDs em Verynims. Em um ambiente real, uma parte publicamente confiável publicaria o DID da RA, declarando que confia que o DID publicado seja o DID público da RA.

Python foi escolhida para ser a principal linguagem de programação para o desenvolvimento. Os motivos para esta escolha foram a documentação do Hyperledger Indy ter sido feita em sua maioria para Python, além da maior experiência e familiaridade do desenvolvedor com esta linguagem. O protótipo então foi programado no formato de um aplicativo web usando a biblioteca Flask (PALLETS, 2010). Esta é uma biblioteca em Python para o desenvolvimento de aplicações web que se utilizam de comunicação HTTP para seu funcionamento.

O protótipo então foi elaborado utilizando uma estratégia baseada em Model-View-Controller (MODEL..., 2009), onde uma parte do sistema cuida da apresentação, outra da interação e outra dos cálculos e manipulação de dados. O protótipo desenvolvido possui um arquivo que contém toda a lógica da visualização e interação do sistema. Este arquivo se utiliza da biblioteca Flask para declarar os pontos de acesso e URL's do sistema. Estes pontos de acesso permitem que através de uma conexão autenticada de um navegador seja possível criar DIDs, Schemas, Definições e Credenciais além de enviar requisições de credenciais e provas.

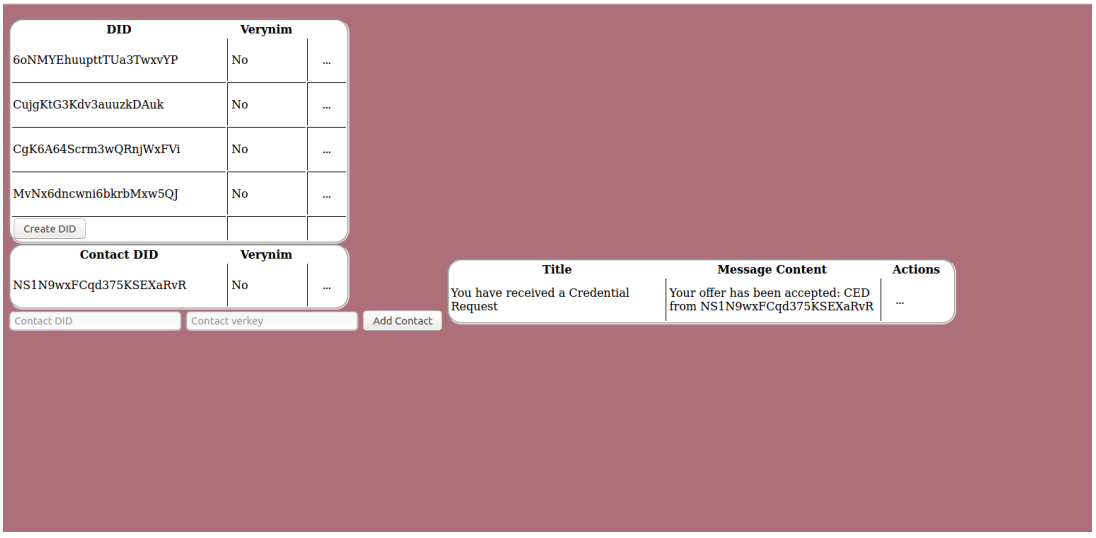

Figura 4 – Demonstração da interface do protótipo desenvolvido

Como o canal de comunicação seguro não faz parte do escopo deste trabalho, uma forma de simular este canal foi a utilização de um banco de dados, como canal e sistema de mensagens, além do próprio sistema de armazenamento do protótipo, armazenando dados do usuário como o identificador de sua wallet, seus dids e seus contatos. Cada instância sepa-

rada do software do protocolo em execução faz a conexão com o banco de dados para realizar a comunicação com a outra instância. O banco de dados então foi esquematizado com tabelas para armazenar os contatos cadastrados de um usuário (contatos), os próprios usuários do sistema (users), seus did's (user_dids), o identificador de sua wallet (wallets), schemas e definições criados (schema_defs), os tipos de mensagens (message_types), os fluxos de credenciais (credential_flow) e as mensagens em si (messages).

A tabela credential_flow é apenas utilizada para auxiliar o fluxo de entrega de uma credencial, ela garante que cada credencial siga um fluxo único. A tabela users é utilizada para armazenar os usuários do sistema, e dependendo de como seria a implementação do sistema, poderia ser utilizada para armazenar os dados de login dos usuários em seus aplicativos, e até permitir a recuperação das credenciais do usuário em caso de perda. A tabela Wallet é utilizada para ligar o usuário ao identificador de sua wallet. No sistema Hyperledger a wallet fica armazenada em um arquivo separado, e no mesmo sistema podem existir mais de uma wallet. A tabela user_dids é utilizada para ligar um usuário aos seus dids. Em uma implementação do sistema esta tabela poderia existir apenas no dispositivo do usuário, ou dependendo de como for desenhado um sistema de recuperação de credenciais, poderia existir em servidores distribuídos, a fim de recuperar as credenciais já emitidas.

As tabelas schema_defs é utilizada para realizar a busca dos schemas e definições na ledger para o fluxo de criação de uma credencial e a tabela message_types para armazenar os tipos de mensagens possíveis. Por fim a tabela messages armazena todas as mensagens enviadas entre usuários. As mensagens podem ser simples comunicações, ou podem possuir objetos como requisições de credenciais e as próprias credenciais. Estas mensagens possuem remetente e destinatário, e em um sistema real teriam um canal de comunicação seguro para serem enviadas. O sistema então permite ao destinatário opções sobre o que fazer com a mensagem dependendo de seu tipo, por exemplo aceitar uma oferta de credencial enviando uma requisição de credencial como resposta, ou aceitar uma credencial oferecida, adicionando-a em sua wallet.

O protótipo então permite que uma instância com o login de um usuário envia mensagens a outra instância hospedada na mesma máquina através deste banco de dados. A instância atualiza as mensagens recebidas ao se recarregar a página principal, e permite realizar ações dependendo do tipo de mensagem recebida. O fluxo do protótipo começa com o a criação do schema e da credencial na página mostrada na figura 5.

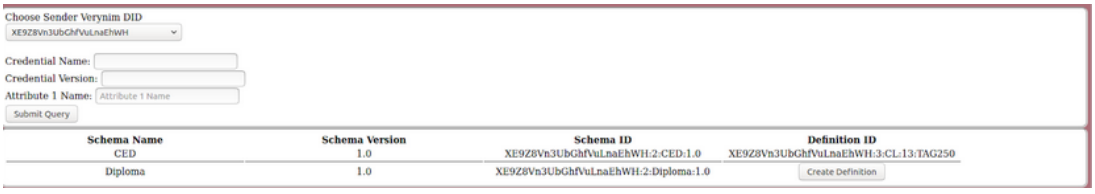

Figura 5 – Demonstração da interface de criação e manutenção de schemas e definições de credenciais.

Depois de criados o schema e a definição, é possível iniciar o fluxo de credenciais. Para esta parte não foi desenvolvida interface para dar foco à funcionalidade. Para realizar o fluxo da credencial, o emissor da credencial deve emitir uma oferta de credencial contendo

o emissor, o destinatário e qual a credencial que se está oferecendo através de uma chamada HTTP direta à aplicação. As outras partes do fluxo podem ser efetuadas a partir da interface, onde o destinatário então aceita a oferta enviando uma requisição de credencial. O emissor por fim gera e envia a credencial para o destinatário que agrega a credencial a sua wallet.

Também não há interface para realizar parte da prova da credencial, neste caso é necessário enviar as requisições HTTP diretamente para a aplicação com a mensagem desejada. A primeira mensagem é a requisição de prova, esta que possui como dados as asserções e os schemas das credenciais que se desejam validar. A resposta pode ser feita através da interface gráfica, onde é necessário escolher as credenciais que preenchem os requisitos da requisição para construir e responder com a prova. A própria biblioteca trás a funcionalidade de se realizar a prova por meio de Zero Knowledge Proofs. Asserções que não sejam comparações diretas de igualdade, podem ser obscurecidas pela própria biblioteca. A prova então pode ser executada sendo comparada com a requisição de prova para ser validada, e a própria biblioteca oferece uma forma de realizar essa prova.

6 DISCUSSÕES

Self-Sovereign Identity é um conceito que traz a identidade de uma pessoa para suas mãos. Isto traz não só o poder, mas também as responsabilidades sobre sua identidade.

Este trabalho traz uma análise das vantagens e desvantagens de SSI e uma forma de implementá-lo em um ambiente real, além de um protótipo e uma análise sobre o protocolo proposto.

Alguns pontos ainda assim se tornam aparentes. Como explicitado, o canal de comunicação não é o foco deste trabalho. A forma de como as credenciais e informações transitam entre usuários e instituições é um ponto importante do funcionamento do sistema. Nos documentos do Hyperledger Indy é mencionado o uso de canais seguros para estas trocas de mensagens (HYPERLEDGER FOUNDATION, 2018). O Hyperledger Aries, um outro projeto sendo desenvolvido pela Fundação Hyperledger visa a construção de aplicações para o compartilhamento das credenciais, e tem como um dos focos a criação destes canais seguros (HYPERLEDGER FOUNDATION, 2019). Outras aplicações encontradas nos trabalhos correlatos também tem como foco o compartilhamento das credenciais (LIU, 2020).

Isto se ligaria com a proposta ao deixar a comunicação mais segura e prática, fortalecendo o objetivo de enviar, receber e verificar as credenciais de qualquer lugar, a qualquer hora. Um canal de comunicação seguro bem definido deixaria o design mais robusto e resistente a ataques, mesmo que ao custo de cerimônias mais complexas ou maior latência entre as mensagens.

O protótipo construído mostra a viabilidade do protocolo, porém por ser um programa mínimo, não tem a capacidade de realizar os testes de carga necessários que uma aplicação que funcionaria a nível nacional sofreria. Outro ponto é que a interface foi deixada como um ponto secundário do desenvolvimento, deixando foco para o funcionamento. Um estudo como o de (ASIRI, 2020) poderia também ser útil para analisar a aceitação deste sistema entre os alunos de universidades.

A retrocompatibilidade é outro ponto de discussão importante e maior contribuição esperada deste trabalho. Como parte do protocolo, a retrocompatibilidade exige que um documento que não faz parte do sistema seja integrado. Desta forma este documento obrigatoriamente não passará por alguma etapa do processo. Um exemplo é um diploma digital sem histórico. A emissão deste documento no sistema em SSI não teria os passos de coleção e verificação do histórico escolar do aluno, sendo apenas validado e reemitido diretamente. Esta característica implica em um foco na segurança desta verificação do documento, a fim de garantir sua validade e veracidade.

Para realizar esta verificação dependendo do sistema origem do documento legado, é necessária colaboração do órgão emissor do documento legado. No caso de diplomas em papel, é possível obter a validação com a instituição de ensino superior que emitiu o documento, ou então como proposto no capítulo 4.4, a existência de entidades notariais que fariam esta verificação. Também podemos citar os portais de conversão de documentos, estes que seriam

integrações entre o sistema legado e o sistema proposto. Como exemplo o diploma digital do MEC, onde seria necessária a colaboração com o MEC para poder criar uma integração que valide e emita o diploma no sistema proposto em SSI.

Esta forma de inserir a retrocompatibilidade no sistema é válida para diversas outras formas de se armazenar documentos digitais. Embora, na pesquisa realizada, nenhum trabalho tenha citado explicitamente como seria uma migração de documentos gerados em outras plataformas, é de se esperar que seja possível realizar a retrocompatibilidade utilizando as formas trazidas no protocolo proposto, com os programas e aplicações trazidos nos trabalhos encontrados.

Por ser baseado na blockchain o sistema é inerentemente distribuído e pode ser implementado com menores custos, dividindo a carga de serviço em vários servidores ao redor do país em que for implementado. Isto também trás o benefício de diminuir a latência aparente para o usuário final. O sistema pode usar uma abordagem híbrida em relação a blockchain, onde usuários comuns operariam de forma anônima, já instituições que possuem seus DIDs publicados poderiam operar de forma privada. Isto faria com que somente usuários privados como as instituições possam criar e distribuir credenciais.

No caso da implementação do sistema, por ser um sistema de natureza híbrida, uma autoridade reguladora, ou conjunto de instituições poderiam ser responsabilizadas pela manutenção do sistema. Esta responsabilidade, dependendo do escopo da aplicação pode ser dada a autoridade reguladora das instituições de ensino, no caso do Brasil o MEC, ou ao governo do país, tendo em vista a escalabilidade do sistema para poder operar com outros tipos de documentos.

A carteira (wallet) onde as informações são guardadas também por si só é um instrumento importante do protocolo. Esta carteira não pode apenas existir no computador pessoal do usuário, deve ser trasportável e utilizável em qualquer lugar. Diversos tipos de técnologia de armazenamento podem ser utilizadas como Hardware para a Wallet. (LóPEZ, 2020) cita os PAD's ou Personal Authentication Devices. Estes dispositivos já são utilizados hoje em dia para controle de transações de criptomoedas, e funcionam como aparelhos dedicados ao armazenamento de chaves e senhas, que podem ou não possuir uma tela ou botões atrelados para sua interação.

A função base do PAD é autenticar as transações de criptomoedas utilizando as chaves neles armazenadas, e protegê-las, evitando que sejam obtidas por usuários maliciosos. Para SSI, dependendo da forma de implementação, e de como essas informações podem ser lidas e carregadas consigo, o PAD pode ser desde um SmartCard, um cartão que possui um chip de processamento interno, que contenha as informações de sua Wallet como um aparelho dedicado ou até estar integrada ao SmartFone pessoal. No caso do SmartCard, pesquisas até já forma feitas para realizar a autorização de transações através de um leitor de digitais integrado ao cartão (SAITO, 2017).

Uma dificuldade encontrada ao se elaborar a análise do protocolo foi a grande porcentagem de interação humana. A entrega de uma Credencial, dependendo da situação pode exigir

a presença in loco do usuário. Desta forma, a comunicação entre a entidade emissora da Credencial e a Wallet do usuário poderiam também ocorrer através de canais secundários e seguros. No caso da Wallet em formato de SmartCard, a interação poderia ocorrer com uma leitora que permita a troca de informações entre o cartão e a instituição. Em PAD's que permitam conexões com a internet, uma aplicação dedicada poderia ser utilizada para receber a credencial de qualquer lugar, a qualquer hora, e também para criar provas e verificá-las. Uma desvantagem do cartão seria a exigência de um aparelho no qual o conectar.

Por possuir partes onde a interação humana é necessária como interfaces de usuário e a necessidade de um humano tomar as ações de enviar as mensagens e decidir quais dados compartilhar, este protocolo se encaixa como um tipo de cerimônia (MARTINA; CARLOS, 2010). Analisá-lo não como um protocolo, mas como uma cerimônia pode trazer mais informações sobre sua segurança levando em conta os fatores humanos.

Como dito antes, SSI traz também a responsabilidade sobre a credencial para o usuário. É possível que uma parte dos usuários não se adaptem à tecnologia, o que pode ocasionar a perda da Wallet ou de suas chaves, sendo então necessárias formas de recuperar as credenciais. Serviços terceiros poderiam ser contratados para o armazenamento de backups, ou estes poderiam ser feitos pelo próprio usuário regularmente. (MARAM et al., 2021) traz uma forma de armazenamento de backup utilizando o próprio sistema proposto, onde as chaves são armazenadas em partes separadas e criptografadas no que os autores chamam de comitê, a recuperação exigiria na prova de que o usuário é quem é, e então na consulta e remontagem dos backups.

Porém estas formas de remontagem dos backups teriam de ter uma atenção especial quanto a segurança. Uma forma comum de roubo de informações e identidade é o Phishing (JANSSON; SOLMS, 2013). Por meio deste golpe, é possível obter as informações de um usuário e se passar por ele com sucesso em frente a um serviço de recuperação de credenciais por exemplo, obtendo assim acesso a Wallet do usuário.

O protocolo propõe a existência da credencial de Permissão de Emissão de diploma (CED), dada por uma autoridade Reguladora (RA), por exemplo o MEC no Brasil, para uma Instituição de Ensino Superior (HEI). Caso um verificador queira ter certeza que um diploma foi emitido por uma instituição válida, ele deve realizar a requisição de prova para a instituição. Uma forma de facilitar este passo seria um aprimoramento do desenvolvimento da tecnologia, ao enviar uma prova genérica, que pode ser executada por qualquer usuário, juntamente com a credencial de diploma. Esta seria uma prova criada pela HEI sobre a CED, e um aluno que receba a requisição de prova de um verificador pode enviá-la juntamente com o diploma, o que permite ao verificador aferi-la sem a necessidade de envolver a HEI.

Uma outra forma de remover a necessidade de envolvimento da HEI seria como mostrado por (LóPEZ, 2020) tendo publicados na blockchain os timestamps de emissão das credenciais. O funcionamento do Hyperledger Indy envolve a blockchain apenas para a publicação de Identificadores Digitais (DID), Schemas e Definições de Credenciais. O aprimoramento envolve a ligação entre uma credencial emitida, por meio de seu identificador único, com o possuidor da credencial por meio de seu DID.

Essa publicação seria feita na blockchain, tornando-a pública e imutável. Este objeto publicado teria como seu conteúdo principal o identificador único da credencial, que não traria informações de seu conteúdo, podendo ser um DID próprio da credencial, juntamente com os DIDs do possuidor e do emissor, mantendo a identidade do possuidor segura, e ainda assim atestando que a credencial foi efetivamente emitida para o seu destinatário

Outras informações poderiam ser adicionadas a esta publicação para aumentar sua utilidade, como o estado de revogação da Credencial ou endereço de um arquivo de revogação, um timestamp da emissão, e possivelmente sua validade. Estes dados atestariam a validade da Credencial para qualquer um que queira verificar. Por fim, este arquivo seria então assinado digitalmente pela instituição emissora, garantindo que quem enviou seja mesmo a instituição cujo DID está na blockchain. Isso permite ao verificador pesquisar na blockchain pelo registro de emissão e verificar se a credencial atribuída à instituição ainda é válida, mesmo sem saber de nenhuma informação publicada na credencial em si.

Um último ponto a ser discutido se trata das revogações dos diplomas emitidos pelo sistema. Por mais seguro que um sistema possa ser, um nodo mal-intencionado pode vir a emitir e distribuir credenciais ilegais, ou então um simples erro humano pode preencher um dado incorretamente em uma credencial. Nesses casos, é necessário que seja possível revogar uma credencial já emitida. O próprio Hyperledger Indy já trás uma forma de implementar a revogação das credenciais emitidas. Quando se é definida uma credencial, esta definição pode levar consigo um endereço de um repositório de revogação.

A partir da credencial é possível obter sua definição pública, e da definição é possível obter o endereço do repositório de revogação, com isso basta consultar o repositório para verificar se a credencial foi revogada. A instituição emissora toma responsabilidade de administrar esse repositório e cada instituição que crie uma definição de uma credencial pode possuir o seu próprio repositório. (VIDAL; GOUVEIA; SOARES, 2020b) trás uma proposta onde ao ser criada e distribuída uma credencial, é gerado um endereço da blockchain relativo a esta credencial, e o estado de revogação é dado se este endereço possui ou não um balanço em moeda. Isto também se interliga com a discussão sobre o que armazenar na blockchain sobre uma credencial, onde o estado de revogação poderia ser um dos dados, além de sua validade, no caso de documentos que necessitem ser renovados periodicamente.

Em suma, embora o protocolo preveja grande parte da interação do usuário com o sistema, alguns pontos ainda devem ser discutidos com relação a sua implementação. Destes os mais importantes são os canais de comunicação, e recuperação dos dados em caso de perdas. Em uma implementação do sistema, a retrocompatibilidade inevitavelmente exigiria a colaboração das partes criadoras da tecnologia legada, juntamente com as formas de verificação destes documentos legados, a fim de garantir sua veracidade. O canal de comunicação depende também de como seria armazenada a Wallet. Uma solução possível e um exemplo seria a utilização dos Smartfones e seus aplicativos para o desenvolvimento do sistema e armazenamento da Wallet. Desta forma, canais de comunicação seguros, e bem definidos devem ser estabelecidos para o envio dos dados e credenciais.

7 CONCLUSÕES

Neste trabalho foi realizada uma revisão da literatura acerca de documentação digital e Self Sovereign Identity, então foi desenvolvido um protocolo para a implementação de um sistema de emissão e verificação de diplomas digitais utilizando SSI e por fim foi construído um protótipo que executa este protocolo para validar sua viabilidade. Como visto na pesquisa realizada, a documentação digital juntamente com SSI é um caminho propício para evitar falsificações de documentos e roubo de identidades. O protocolo proposto trás uma forma de implementação desta tecnologia, trazendo a discussão para a retrocompatibilidade com sistemas legados, e o protótipo desenvolvido demonstra a viabilidade deste protocolo. As vantagens do protocolo proposto estão no próprio uso do SSI, que herda as qualidades da Blockchain e trás a responsabilidade dos dados para o próprio usuário. Outra vantagem é a retrocompatibilidade, que facilitaria a conversão de documentos existentes para o sistema proposto, trazendo assim um número maior de usuários, devido a acessibilidade, embora este ponto deva ser tratado com cautela, a fim de não criar vulnerabilidades no sistema e permitir que documentos falsos sejam criados em tecnologias legadas e convertidos ao novo sistema.

8 TRABALHOS FUTUROS

Como trabalhos futuros, um estudo sobre a legislação Brasileira deve ser feito, a fim de adequar o protocolo às cerimônias legais necessárias, antes da criação de qualquer protótipo, além de garantir que este sistema estará de acordo com a Lei Geral de Proteção de Dados brasileira. Outra via de trabalho paralela antes da implementação deste protocolo é a sua verificação utilizando ferramentas formais de verificação de protocolos e cerimônias, o que sem dúvida determinará sua eficácia e segurança. Há também a necessidade de estudar as formas de assegurar que os documentos legados são verídicos, antes de serem convertidos a tecnologia proposta, e de estudar as formas de criar portais e entidades que possam realizar estas validações de forma oficial.

REFERÊNCIAS

ABREU, A. W. S.; COUTINHO, E. F.; BEZERRA, C. I. A blockchain-based architecture for query and registration of student degree certificates. In: **SBCARS '20**. [S.l.: s.n.], 2020. p. 151–160.

ALLEN, C. **The Path to Self-Sovereign Identity**. 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-selfsoverereign-identity.html.

ARENAS, R.; FERNANDEZ, P. Credenceledger: A permissioned blockchain for verifiable academic credentials. In: IEEE. **ICE/ITMC**. [S.l.], 2018. p. 1–6.

ASIRI, L. **Blockchain For Educational Certificate Distribution**. Tese (Doutorado) — Florida Institute of Technology, 2020.

ATAŞEN, K.; ASLAN, B. A blockchain based digital certification platform: Certidapp. **(JMEST**, 2020.

AVERIN, A.; SNEGIREVA, D.; LADEJSHCHIKOV, A. Model of a monitoring system for academic performance and the issuance of diplomas using blockchain technology. In: IEEE. **IT&QM&IS**. [S.l.], 2020. p. 88–91.

BAHRAMI, M.; MOVAHEDIAN, A.; DELDARI, A. A comprehensive blockchain-based solution for academic certificates management using smart contracts. In: IEEE. **2020 10th ICCKE**. [S.l.], 2020. p. 573–578.

BHUMICHITR, K.; CHANNARUKUL, S. Acachain: Academic credential attestation system using blockchain. In: **IAIT2020**. [S.l.: s.n.], 2020. p. 1–8.

BRASILEIRO, M. de E. **10665 - Projeto Jornada do Estudante e MVP da Rede Aprender**. 2021. Disponível em: http://simec.mec.gov.br/ted/termo-de-execucao-descentralizada.php.

BRUNNER, C.; KNIRSCH, F.; ENGEL, D. Sproof: A platform for issuing and verifying documents in a public blockchain. In: **ICISSP**. [S.l.: s.n.], 2019. p. 15–25.

BUDHIRAJA, S.; RANI, R. Tudocchain-securing academic certificate digitally on blockchain. In: SPRINGER. **ICICIT**. [S.l.], 2019. p. 150–160.

CASTRO, R. Q.; AU-YONG-OLIVEIRA, M. Blockchain and higher education diplomas. **European Journal of Investigation in Health, Psychology and Education**, Multidisciplinary Digital Publishing Institute, v. 11, n. 1, p. 154–167, 2021.

ČEKE, D.; KUNOSIĆ, S. Smart contracts as a diploma anti-forgery system in higher education-a pilot project. In: IEEE. **MIPRO**. [S.l.], 2020. p. 1662–1667.

CHENG, H. e. a. A permissioned blockchain-based platform for education certificate verification. In: SPRINGER. **BlockSys**. [S.l.], 2020. p. 456–471.

DAVIDGOTHBERG. **Hash Function**. 2005. Public domain, via Wikimedia CommonsURL. Disponível em: https://upload.wikimedia.org/wikipedia/commons/d/da/Hash_function.svg.

DHONGADE, R. **Blockchain**. 2019. Disponível em: https://www.spheregen.com/wp-content/uploads/2019/04/blockchain.png.

DIMA, G.-A. et al. Scholarium: Supporting identity claims through a permissioned blockchain. In: IEEE. **RTSI**. [S.l.], 2018. p. 1–6.

DOUCEUR, J. R. The sybil attack. In: SPRINGER. **International workshop on peer-to-peer systems**. [S.l.], 2002. p. 251–260.

DURANT, E.; TRACHY, A. **Digital Diploma debuts at MIT. Using Bitcoin's blockchain technology, the Institute has become one of the first universities to issue recipient-owned virtual credentials**. 2017.

FORTNOW, L. The complexity of perfect zero-knowledge. In: **STOC '87**. New York, New York: [s.n.], 1987. p. 204–209.

GHAZALI, O.; SALEH, O. S. A graduation certificate verification model via utilization of the blockchain technology. **JTEC**, v. 10, n. 3-2, p. 29–34, 2018.

GLOBO G1 CE. **Alunos pagavam até R$ 3 mil por diploma falso emitido por faculdade no Ceará**. 2021. https://g1.globo.com/ce/ceara/noticia/2021/05/11/alunos-pagavam-ate-r-3-mil-por-diploma-falsoemitido-por-faculdade-no-ceara.ghtml.

GOVERNO BRASILEIRO. **PROVISORIA No 2.200-2, DE 24 DE AGOSTO DE 2001.** 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm.

HAN, M. e. a. A novel blockchain-based education records verification solution. In: **SIGITE '18**. [S.l.: s.n.], 2018. p. 178–183.

HYPERLEDGER FOUNDATION. **Hyperledger**. 2015. Disponível em: https://www.hyperledger.org/.

HYPERLEDGER FOUNDATION. **Hyperledger Indy**. 2018. Disponível em: https://www.hyperledger.org/use/hyperledger-indy.

HYPERLEDGER FOUNDATION. **Hyperledger Aries**. 2019. Disponível em: https://www.hyperledger.org/use/aries.

JAKOBSSON, M.; JUELS, A. Proofs of work and bread pudding protocols. In: **Secure information networks**. [S.l.]: Springer, 1999. p. 258–272.

JANSSON, K.; SOLMS, R. von. Phishing for phishing awareness. **Behaviour & Information Technology**, Taylor & Francis, v. 32, n. 6, p. 584–593, 2013. Disponível em: https://doi.org/10.1080/0144929X.2011.632650.

KALTYSHEV, M. **Proof of university certificate using blockchain technology**. Tese (Doutorado) — Häme University of Applied Sciences, 2018.

LEKA, E.; SELIMI, B. Bcert–a decentralized academic certificate system distribution using blockchain technology. **International Journal on Information Technologies & Security**, v. 12, n. 4, 2020.

LEPIANE, C. D. et al. Digital degree certificates for higher education in brazil: A technical policy specification. In: **DocEng '19**. [S.l.: s.n.], 2019. p. 1–10.

LIU, D.; GUO, X. Blockchain based storage and verification scheme of credible degree certificate. In: IEEE. **IICSPI**. [S.l.], 2019. p. 350–352.

LIU, Y. e. a. Blockchain-based identity management systems: A review. **Journal of network and computer applications**, Elsevier, v. 166, p. 102731, 2020.

LóPEZ, M. A. **Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain**. 2020. https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignitydigital-wallets-and-blockchain.

MARAM, D. et al. Candid: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability. In: IEEE. **2021 IEEE Symposium on Security and Privacy (SP)**. [S.l.], 2021. p. 1348–1366.

MARTINA, J. E.; CARLOS, M. C. Why should we analyse security ceremonies. **Proc. of CryptoForma**, 2010.

MERKLE, R. C. **Method of providing digital signatures**. [S.l.]: Google Patents, 1982. US Patent 4,309,569.

MINISTÉRIO DA EDUCAÇÃO BRASILEIRO. **Diploma Digital**. 2018. Disponível em: http://portal.mec.gov.br/diplomadigital/#sobre.

MIT MEDIA LABS. **Blockcerts-An Open Infrastructure for Academic Credentials on the Blockchain**. 2016. Disponível em: https://www.blockcerts.org/about.html.

MODEL View Controller Pattern. In: LEARN Objective-C for Java Developers. Berkeley, CA: Apress, 2009. p. 353–402. ISBN 978-1-4302-2370-2. Disponível em: https://doi.org/10.1007/978-1-4302-2370-2_20.

MOHANTA, B. K.; PANDA, S. S.; JENA, D. An overview of smart contract and use cases in blockchain technology. In: IEEE. **2018 9th international conference on computing, communication and networking technologies (ICCCNT)**. [S.l.], 2018. p. 1–4.

MORISIO, M.; ARDITO, L.; YOKUBOV, B. **Blockchain based storage of students career**. Tese (Doutorado) — Politecnico di Torino, 2018.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. https://bitcoin.org/bitcoin.pdf.

NGUYEN, D.-H. et al. Cvss: a blockchainized certificate verifying support system. In: **SoICT 2018**. [S.l.: s.n.], 2018. p. 436–442.

PALLETS. **Python Flask**. 2010. Disponível em: https://flask.palletsprojects.com/en/2.2.x.

PALMA, L. M. et al. Blockchain and smart contracts for higher education registry in brazil. **International Journal of Network Management**, Wiley Online Library, v. 29, n. 3, p. e2061, 2019.

PALMA, L. M. d. et al. Blockchain-based academic record system. 2020.

PATEL, D. e. a. Issuing and verifying university certificates on blockchain. In: **IC-BCT 2019**. [S.l.]: Springer, 2020. p. 79–91.

PEREIRA, F. L. et al. **Perspectivas para o desenvolvimento e implantação de um sistema de emissão de diplomas baseado em certificação digital na Universidade Federal de Santa Catarina-UFSC**. Tese (Doutorado) — Universidade Federal de Santa Catarina, 2015.

PETRE, L.-C.; PAQUE, B.; LEJEUNE, C. **What are the potential benefits of blockchain applications for the Université Catholique de Louvain?** Tese (Doutorado) — Louvain School of Management, 2019.

PILKINGTON, M. Blockchain technology: principles and applications. In: **Research handbook on digital transformations**. [S.l.]: Edward Elgar Publishing, 2016.

PRENEEL, B. Cryptographic hash functions. **European Transactions on Telecommunications**, Wiley Online Library, v. 5, n. 4, p. 431–448, 1994.

PROTOCOL LABS. **InterPlanetary File System. GitHub repository.** 2020. https://github.com/ipfs/ipfs.

RAVAL, S. **Decentralized applications: harnessing Bitcoin's blockchain technology**. [S.l.]: "O'Reilly Media, Inc.", 2016.

SAITO, T. **Smart card for passport, electronic passport, and method, system, and apparatus for authenticating person holding smart card or electronic passport**. [S.l.]: Google Patents, 2017. US Patent App. 14/533,388.

SAN, A. M.; CHOTIKAKAMTHORN, N.; SATHITWIRIYAWONG, C. Blockchain-based learning credential verification system with recipient privacy control. In: IEEE. **TALE**. [S.l.], 2019. p. 1–5.

SAYED, R. H. **Potential of blockchain technology to solve fake diploma problem**. Tese (Doutorado) — University of Jyväskylä, 2019.

SCHÄR, F.; MÖSLI, F. Blockchain diplomas: Using smart contracts to secure academic credentials. **Journal of Higher Education Research**, v. 41, n. 3, p. 48–58, 2019.

SZABO, N. Formalizing and securing relationships on public networks. **First monday**, 1997.

THE SOVRIN FOUNDATION. **Sovrin**. 2018. Disponível em: https://sovrin.org/.

VIDAL, F. R.; GOUVEIA, F.; SOARES, C. Blockchain application in higher education diploma management and results analysis. **ASTES**, 2020.

VIDAL, F. R.; GOUVEIA, F.; SOARES, C. Revocation mechanisms for academic certificates stored on a blockchain. In: IEEE. **2020 15th CISTI**. [S.l.], 2020. p. 1–6.

WONG, J. I. **University of Nicosia Issues Block-Chain Verified Certificates**. 2014. Disponível em: https://www.coindesk.com/university-nicosia-issuesblock-chain-verified-certificates.

WOOD, G. et al. Ethereum: A secure decentralised generalised transaction ledger. **Ethereum project yellow paper**, v. 151, n. 2014, p. 1–32, 2014.

YEH, L.-Y. e. a. E-university applications: A privacy-preserving diploma notarization platform in taiwan. In: **EEE**. [S.l.: s.n.], 2018. p. 44–50.

APÊNDICE A – EXECUÇÃO DO PROTOCOLO

Algumas notas a serem consideradas antes da execução são:

Hashes, Digests e números de verificação foram omitidos, pois são calculados pela biblioteca, para simplificar os Payloads.

A autorização da HEI pela RA tem duas etapas, primeiro a RA deve publicar o verynim da HEI. Em seguida, deve emitir um CED (Credencial para a Emissão de diplomas) e entregá-lo à HEI. Dessa forma, a HEI pode criar provas de que é uma instituição válida.

O RA cria um Verynim para HEI enviando o payload mostrado no listing A.1 para a ledger

Listing A.1 – Payload de Formalização de Verynim

```
{
    "reqId": 1633959591293384200,
    "identifier": "RA DID",
    "operation": {
        "type": 1,
        "dest": "HEI DID",
        "verkey": "HEI VERKEY",
        "role": 101
    },
    "protocolVersion": 2
}
```

Se a solicitação for um sucesso, a ledger responde com o payload e o verynim do listing A.2

Listing A.2 – Payload de retorno do cadastro de Verynim

```
{
  "op": "REPLY",
  "result": {
    "txn": {
      "type": "1",
      "data": {
        "verkey": "HEI VERKEY",
        "role": "101",
        "dest": "HEI DID"
      },
      "protocolVersion": 2,
      "metadata": {
        "reqId": 1633959591293384200,
        "digest": "...",
```

```
        "from": "RA DID",
        "payloadDigest": "..."
      }
    },
    "ver": "1",
    "rootHash": "...",
    "auditPath": [
      "..."
    ],
    "reqSignature": {
      "type": "ED25519",
      "values": [
        {
          "from": "RA DID",
          "value": "..."
        }
      ]
    },
    "txnMetadata": {
      "seqNo": 19,
      "txnId": "...",
      "txnTime": 1633959591
    }
  }
}
```

Depois que o DID for publicado na ledger, é possível ser consultado enviando o payload descrito no listing A.3 para a ledger:

Listing A.3 – Payload de consulta de um Verynim

```

{
  "reqId": 1633959592954349800,
  "identifier": "LibindyDid111111111111",
  "operation": {
    "type": "105",
    "dest": "REQUESTED DID"
  },
  "protocolVersion": 2
}
```

Se o DID existir na ledger, o payload resultante será o que é apresentado no listing A.4

Listing A.4 – Payload de um retorno da consulta de um Verynim

```
{
  "op": "REPLY",
  "result": {
    "dest": "REQUESTED DID",
    "data": "{
  "dest": "REQUESTED DID",
  "identifier": "QUERYING DID",
  "role": "101",
  "seqNo": 11,
  "txnTime": 1633881936,
  "verkey": "QUERYING DID VERKEY"
}",
    "state_proof": {
      "proof_nodes": "...",
      "root_hash": "...",
      "multi_signature": {
        "value": {
          "ledger_id": 1,
          "txn_root_hash": "...",
          "state_root_hash": "...",
          "pool_state_root_hash": "...",
          "timestamp": 1633959591
        },
        "participants": [
          "Node4",
          "Node1",
          "Node2"
        ],
        "signature": "..."
      }
    },
    "seqNo": 11,
    "identifier": "LibindyDid111111111111",
    "type": "105",
    "txnTime": 1633881936,
    "reqId": 16339595929543498 00
  }
```

```
}
```

Após o RA publicar o DID da HEI, ele deve criar um Schema e uma Definition para a credencial usada para autorizar as HEI a emitirem diplomas e Credenciais de Disciplinas.

A criação do Schema requer que lhe seja dado um Nome, uma Versão e uma Lista de Atributos. O Schema é então publicado na Ledger com o payload demonstrado no listing A.5

Listing A.5 – Payload de um esquema de credencial

```
{
  "reqId": 1633962392696829400,
  "identifier": "RA DID",
  "operation": {
    "type": "101",
    "data": {
      "name": "CED",
      "version": "2.0",
      "attr_names": [
        "Issuer DID",
        "University DID",
        "Expiry Date",
        "University Name"
      ]
    }
  },
  "protocolVersion": 2
}
```

Como o RA é quem está emitindo as credenciais do CED, o RA precisa publicar uma Credential Definition na ledger, enviando o payload do listing A.6. Essa Definition contém metadados sobre a credencial, como se ela oferece suporte à revogação. Caso isso aconteça, o registro de revogação deve ser publicado também na ledger, vinculando-o à credencial publicada.

Listing A.6 – Payload de uma definição de credencial

```
{
  "reqId": 1633962615515023400,
  "identifier": "RA DID",
  "operation": {
    "ref": 20,
    "data": {
      "primary": {
        "n": "...",
```

```
        "s": "...",
        "r": {
          "universitydid": "...",
          "expirydate": "...",
          "master\_secret": "...",
          "universityname": "...",
          "issuerdid": "..."
        },
        "rctxt": "...",
        "z": "..."
      }
    },
    "type": "102",
    "signature\_type": "CL",
    "tag": "TAG26"
  },
  "protocolVersion": 2
}
```

Depois de publicar o Schema e a Definition não é necessário enviar mais nada à Ledger. O RA pode então oferecer uma credencial à HEI, tomando como base o Schema e Definition criados, como mostra o listing A.7. Essa carga contém dados sobre a credencial que está sendo oferecida. Essas trocas devem ser enviadas por meio de canais seguros e nunca são publicadas no ledger ou em qualquer outro lugar.

Listing A.7 – Payload de uma oferta de credencial

```
{
  "cred_def_id": "CREDENTIAL DEFINITION ID",
  "nonce": "606851816570916812006484",
  "key_correctness_proof": {
    "xr\_cap": [
      [
        "master_secret",
        "..."
      ],
      [
        "universityname",
        "..."
      ],
      [
        "issuerdid",
```

```
        "..."
      ],
      [
        "universitydid",
        "..."
      ],
      [
        "expirydate",
        "..."
      ]
    ],
    "xz_cap": "...",
    "c": "..."
  },
  "schema_id": "CujgKtG3Kdv3auuzkDAuk:2:CED:2.0"
}
```

A HEI com esse payload pode criar uma solicitação de credencial. Isso vincula a Credencial a este DID, tornando-a intransferível, mostrado no listing A.8.

Listing A.8 – Payload de uma requisição de credencial

```
{
  {
    "cred_def_id": "CREDENTIAL DEFINITION ID",
    "prover_did": "RECEIVER DID",
    "nonce": "429187573248791939863829",
    "blinded_ms_correctness_proof":
      {
        "r_caps": {},
        "v_dash_cap": "...",
        "m_caps": {
          "master_secret": "..."
        },
        "c": "..."
      },
    "blinded_ms": {
      "committed_attributes": {},
      "ur": null,
      "hidden_attributes": ["master_secret"],
      "u": "..."
    }
```

```
  },
  "cred_req_metadata_json": {
    "master_secret_blinding_data": {
        "v_prime": "...",
        "vr_prime": null
    },
    "master_secret_name": "...",
    "nonce": "42918757324879193986382 9"
  }
}
```

O RA, após ter recebido o pedido, pode então criar a própria credencial preenchendo os valores de cada atributo e enviando-o à HEI, visto no listing A.9.

Listing A.9 – Payload de uma credencial

```
{
  "values": {
    "University DID": {
      "encoded": "...",
      "raw": "Kxdw7YRR2EVGFG22bv1iAw"
    },
    "Issuer DID": {
      "encoded": "...",
      "raw": "6oNMYEhuupttTUa3TwxvYP"
    },
    "Expiry Date": {
      "encoded": "...",
      "raw": "1641006000"
    },
    "University Name": {
      "encoded": "...",
      "raw": "UFSC"
    }
  },
  "rev_reg": null,
  "witness": null,
  "signature_correctness_proof": {
    "se": "",
    "c": ""
  },
  "rev_reg_id": null,
```

```
  "cred_def_id": "CREDENTIAL DEFINITION ID",
  "schema_id": "CujgKtG3Kdv3auuzkDAuk:2:CED:2.0",
  "signature": {
    "p_credential": {
      "v": "...",
      "a": "...",
      "m_2": "...",
      "e": "..."
    },
    "r_credential": null
  }
}
```

A credencial é então armazenada com segurança na Carteira da HEI. O mesmo processo é feito para as credenciais da Disciplina e do diploma, com algumas ressalvas. Para a credencial de diploma, o RA define quais Cursos uma HEI pode ministrar e cria Schemas de diploma para cada um dos Cursos.

Para este Schema, a HEI é quem os define, pois cada HEI pode ter seus próprios metadados para ela, como seu próprio registro de revogação. Quanto à credencial de Disciplina, a HEI cria tanto o Schema quanto a Definition.

O processo segue então o currículo do aluno. Para cada disciplina que o aluno concluir com notas suficentes para aprovação, ele é recompensado com uma credencial de disciplina pela HEI, emitida com as mesmas etapas da credencial CED. Isso constrói todo o histórico escolar do aluno, e fica armazenado em sua carteira, ou seja, o aluno pode comprovar o conhecimento de um assunto criando uma prova com uma dessas credenciais.

Para ser elegível para receber a credencial do diploma, o aluno receberá uma solicitação de comprovação da HEI. Essa solicitação de prova assume a forma de um arquivo JSON solicitando as credenciais do histórico do aluno. Por exemplo, se a Credencial de completude de uma disciplina tiver os atributos: Nota Média, Nome do aluno e Nome da Disciplina, a solicitação de prova deve requisitar apenas os atributos que se desejam provar, como mostrado no listing A.10, que solicita uma nota 7 (equivalente a um B no sistema de notas por letras) em Cálculo A:

Listing A.10 – Payload de uma requisição de prova

```
{
  "version": "1.0",
  "requested\_predicates": {
    "predicate1\_referent": {
      "p\_value": 7,
      "restrictions": [
        {
```

```
            "issuer\_did": "REQUIRED ISSUER DID",
            "schema\_id": "REQUIRED SCHEMA ID"
          }
        ],
        "p\_type": ">=",
        "name": "Average"
      }
    },
    "name": "Proof Request for Subject",
    "requested\_attributes": {
      "attr1\_referent": {
        "restrictions": [
          {
            "issuer\_did": "REQUIRED ISSUER DID",
            "schema\_id": "REQUIRED SCHEMA ID",
            "attr::subjectname::value": "Calculus A"
          }
        ],
        "name": "Subject Name"
      },
      "attr2\_referent": {
        "restrictions": [
          {
            "issuer\_did": "REQUIRED ISSUER DID",
            "attr::studentname::value": "Luca Fachini Campelli"
              ,
            "schema\_id": "REQUIRED SCHEMA ID"
          }
        ],
        "name": "Student Name"
      }
    },
    "nonce": "887908430547"
}
```

O aluno então selecionaria todas as credenciais válidas de sua carteira para atender à solicitação de prova completa, uma para cada disciplina. Caso o aluno falte uma disciplina, ou a nota média recebida para ela não seja suficiente, o aluno não poderá gerar a prova exigida.

Para gerar a prova, o aluno pode escolher quais atributos deixar revelados. Neste caso, não há razão para esconder seu nome, ou o nome da disciplina. Mas para uma entrevista de

emprego, por exemplo, o aluno pode querer ocultar sua nota exata ou outras informações que possam estar incluídas na credencial. Isso não afeta a prova, mas como restrição, se uma prova solicitar um valor específico, digamos que seu nome seja igual a João, esse atributo deve ser revelado. Não há motivo para ocultar um valor já conhecido, se você estiver solicitando uma igualdade.

O comprovante é então enviado para a HEI que pode verificar se todos os dados revelados estão conforme solicitado e validar o comprovante. Se a prova for válida, a HEI pode emitir a credencial do diploma para o aluno. O diploma agora é de inteira responsabilidade do aluno, e a única parte da informação sobre ele que fica com a HEI deve ser um identificador do documento, caso haja necessidade de revogação.

Essas etapas não são estritamente necessárias para a emissão da credencial de diploma. Por uma questão de compatibilidade com sistemas legados onde o histórico do aluno não está disponível, a credencial de diploma deve poder ser emitida mesmo sem essas credenciais. Uma extensão do protocolo é a existência de entidades notariais. Essas entidades são de confiança pública e têm a função de receber credenciais emitidas em outros sistemas legados, como diplomas em papel, autenticando-os e emitindo-os no formato Digital SSI. Para essas entidades, o histórico do aluno pode ser opcional.

Outra entidade de extensão é a disponibilização de oráculos ou web services desenvolvidos por ou com os emissores das tecnologias legadas. Por exemplo, o MEC do Brasil poderia disponibilizar um serviço web que recebe e valide seus diplomas Digitais e os emita no formato digital SSI. Isso garante que o protocolo seja compatível com sistemas legados e que seja agnóstico com a tecnologia emitida anteriormente.

De posse do diploma, um terceiro verificador, como uma empresa que procura a contratação do aluno, pode emitir um pedido de comprovação do diploma do aluno para verificar suas reivindicações para o processo de contratação. Isso pode ser feito usando o mesmo processo descrito para a prova de diploma.