Protocolo de diploma Digital Auto-Soberano com Retrocompatibilidade Tecnológica

Uma Solução Adaptada a Realidade Brasileira

Luca Campelli[1], **Lucas Palma**[1], **Jean Martina**[1]

[1]Departamento de Informática e Estatística
Programa de Pós-Graduação em Ciências da Computação
Universidade Federal de Santa Catarina

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 monitoring 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. This article 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.*

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 artigo, será 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.*

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, 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. 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].

Além dos trabalhos citados, outros projetos e pesquisas propõem o armazenamento de informações em uma blockchain afim de torná-las verificáveis e resistentes a modificações. Este é o caso da proposta de [Ghazali and 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 et al. 2019] utilizam árvores de Merkle [1] para que vários documentos possam ser publicados na blockchain em uma só transação. [Yeh 2018] foca em armazenar e recuperar o documento utilizando um QR code e dividindo-o em partes que são armazenadas em locais diferentes. Demais trabalhos procuram focar em outros aspectos do processo, como [Vidal et al. 2020b] que foca em estudar a revogação de um documento emitido.

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. 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].

Poucas pesquisas na literatura utilizam SSI como parte fundamental de suas

[1]Estruturas de dados em formato de árvore onde os nodos folha são resumos criptográficos dos arquivos e cada nodo acima é um resumo criptográfico dos resumos criptográficos dos nodos abaixo. O nodo raíz é chamado de raíz de Merkle.[Merkle 1982]

propostas de emissão de diplomas de conclusão de curso e créditos acadêmicos. Alguns trabalhos que adotam a blockchain se aproximam do conceito, porém falham por não cumprir com um ou outro dos dez princípios do SSI, detalhados na seção 2.2 [Durant and Trachy 2017][Petre et al. 2019][Yeh 2018]. Por exemplo, muitos falham em manter a minimalidade das informações que são discorridas, ou falham em se manter transportáveis entre provedores de identidades diferentes. Além disso, uma das tecnologias blockchain utilizada neste artigo, a Hyperledger Indy [Hyperledger Foundation 2018], possui em seus exemplos práticos um caso onde um diploma é emitido por uma instituição e atribuído à um estudante. Este exemplo é genérico pois não leva em conta protocolos e cerimônias existentes, ou legislações necessárias.

O objetivo deste trabalho é propor um protocolo que pode ser utilizado em um ambiente real de uma instituição de ensino superior brasileira, onde todo o processo de emissão do diploma seja considerado, desde os dados de histórico, até a emissão e utilização do documento na prática. Além disso, busca-se 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, pois este, já é utilizado por grandes iniciativas, como é o caso do Sovrin [The Sovrin Foundation 2018].

O restante deste artigo está organizado da seguinte maneira: no capítulo 2 são apresentados conceitos essenciais para a compreensão da proposta, no capítulo 3 são descritos os trabalhos relacionados encontrados na literatura, no capítulo 4, apresenta-se o protocolo desenvolvido e no capítulo 5 são traçadas as considerações finais.

2. Conceitos Preliminares

Nesta seção são apresentados os conceitos e tecnologias utilizados no protocolo proposto na seção 4. Na seção 2.1, discute-se conceitos introdutórios de blockchain e na seção 2.2 introduz-se SSI e seus princípios.

2.1. blockchain

Inicialmente concretizada 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, com $i \in \mathbb{N}$ está ligado ao bloco anterior (B_{i-1}) por meio de um resumo criptográfico, gerado a partir do conteúdo do bloco anterior. 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.

Os usuários da blockchain se mantém conectados em uma rede peer-to-peer, onde as transações e notificações de blocos computados são enviadas e compartilhadas em um sistema distribuído. 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.

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. blockchains privadas exigem que os usuários sejam conhecidos e convidados a participar da geração da cadeia de blocos. Já as blockchains híbridas são a combinação das duas anteriores, podendo operar em parte de forma pública e outra de forma privada [Pilkington 2016].

Além do Bitcoin, vale destacar outras implementações de blockchain como o Ethereum [Wood et al. 2014] e o conjunto de implementações da Hyperledger [Hypeledger 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 de aplicativos decentralizados [Raval 2016].

2.2. Self Sovereign Identity

Self-Sovereign Identity (SSI), é o conceito onde a autoridade 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].

Segundo [Allen 2016], pode-se elencar dez princípios que descrevem SSI:

- **Existência** - A existência do indivíduo deve ser única, e não somente digital;
- **Controle** - Indivíduos devem ter o controle sobre suas identidades, poder atualizá-las, referenciá-las e até escondê-las, além de escolher o quão públicas ela são;
- **Acesso** - O indivíduo deve ter acesso total a sua identidade e poder ver todas as afirmações e dados sobre ela, sem ofuscamento;
- **Transparência** - Sistemas e algoritmos utilizados devem ser transparentes;
- **Persistência** - Identidades devem durar por um logo tempo e se manter válidas até que se tornem desatualizadas por sistemas mais novos;
- **Portabilidade** - Informações e serviços de identidade devem se manter trasportáveis e não serem retidos por apenas um provedor de identidades terceiro;
- **Interoperabilidade** - Identidades devem ser o mais amplamente utilizáveis o quanto possível, podendo serem utilizadas em qualquer lugar;
- **Consentimento** - Indivíduos devem consentir o uso de suas identidades;
- **Minimalização** - Apenas o mínimo necessário de informações deve ser compartilhado;
- **Proteção** - Os direitos dos indivíduos devem ser protegidos. Conflitos devem ser resolvidos de forma que não prejudiquem esses direitos.

O foco de SSI é a privacidade do indivíduo, 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. 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].

3. Trabalhos Relacionados

Para melhor compreender o estado da arte acerca da emissão de diplomas digitais, foi realizada uma revisão sistemática da literatura. Como resultado foram selecionados os trabalhos detalhados nesta seção.

Diversos autores utilizam as tecnologias de blockchain para o armazenamento dos diplomas Digitais, o que garante temporalidade e imutabilidade as informações [Castro and Au-Yong-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. Na Tabela 1 são apresentados os trabalhos relacionados encontrados no processo de revisão, classificados de acordo com os seguintes critérios:

- **Tecnologia Utilizada** - *Qual foi a tecnologia blockchain utilizada para a construção da solução?*
- **Utilização de Smart Contracts** - *A solução proposta utiliza 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 princípios de SSI?*

Trabalho	Tecnologia	Smart Contracts	SSI
[Petre et al. 2019]	Blockcerts	✓	✗
[Bahrami et al. 2020]	Hyperledger Fabric	✓	✗
[Morisio et al. 2018]	Ethereum, ERC20 Tokens	✓	✗
[Durant and Trachy 2017]	Blockcerts	✓	✗
[Liu 2020]	Sovrin, uPort, Shocard	✓	✗.
[Kaltyshev 2018]	Multichain	✗	✗
[Leka and Selimi 2020]	Ethereum	✓	✗
[Han 2018]	Undisclosed	✓	✗
[Abreu et al. 2020]	Ethereum	✓	✗
[Ghazali and Saleh 2018]	Não Especificado	✗	✗
[Vidal et al. 2020b]	Não Especificado	✗	✗
[Patel 2020]	Ethereum	✓	✗
[Brunner et al. 2019]	Não Especificado	✗	✗
[Yeh 2018]	Ethereum	✓	✗
[Palma et al. 2020]	Ethereum	✓	✗
[Ataşen and Aslan 2020]	Ethereum	✓	✗
[Budhiraja and Rani 2019]	Ethereum	✓	✗
[Cheng 2020]	Hyperledger Fabric	✓	✗
[Dima et al. 2018]	Multichain	✗	✗
[Liu and Guo 2019]	Hyperledger Fabric	✗	✗
[Averin et al. 2020]	Não Especificado	✗	✗
[Arenas and Fernandez 2018]	Multichain	✗	✗
[Vidal et al. 2020a]	Blockcerts, Bitcoin, Ethereum	✗	✗
[Schär and Mösli 2019]	Ethereum	✓	✗
[Sayed 2019]	Ethereum	✓	✗
[Bhumichitr and Channarukul 2020]	Hyperledger Fabric	✗	✗
[Nguyen et al. 2018]	Ethereum	✓	✗
[San et al. 2019]	Não Especificado	✗	✗
[Čeke and Kunosić 2020]	Ethereum	✓	✗

Cont. Tabela 1			
Trabalho	Tecnologia	Smart Contracts	SSI
Esse Trabalho	Hyperledger Indy	✗	✓

Tabela 1. Trabalhos Relacionados. O símbolo ✓ demonstra uma entrada positiva, o símbolo ✗ demonstra entradas parciais, e o símbolo ✗ demonstra entradas negativas.

Na Tabela 1 não foram incluídos três trabalhos, por não se encaixarem nos critérios de comparação. [Asiri 2020] trás um estudo demográfico sobre a aceitação dos sistemas de documentação digital em blockchain, mas que é de grande relevância conceitual para a pesquisa apresentada neste artigo. [Castro and Au-Yong-Oliveira 2021] faz uma revisão sistemática apenas na plataforma Scopus, mostrando 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 trás uma solução que se aproxima daquela proposta pelo Ministério da Educação [Ministério da Educação Brasileiro 2018], utilizando a ICP-Brasil e arquivos XML, porém utilizando sistemas de arquivos distribuídos para o armazenamento.

Para além da classificação, uma análise dos trabalhos apresentados na Tabela 1 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.

Entre os pontos positivos da adoção da blockchain, pode-se destacar que, por ser um sistema distribuído, não possui um só ponto de falha, além de trazer registros ordenados, com timestamps, o que aumenta a quantidade de informação possível de ser resgatada e verificada. Além disso, após um certo número de transações, os registros são considerados imutáveis e publicamente verificáveis nas blockchains públicas.

Outra vantagem é a automatização, com Smart Contracts. Como mostrado em [Nguyen et al. 2018], [Vidal et al. 2020a], e [Ataşen and 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.

[López 2020] trás alguns dos benefícios que SSI trás para a documentação digital, como interoperabilidade, pseudonimidade, pertencibilidade, portabilidade, recuperação, escalabilidade e segurança. SSI também trás vantagens pelo seu funcionamento intrínseco na blockchain, possuindo 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 deixar de existir devido a falência. [Tokarnia 2014]

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 informações não essenciais são discorridas. Alguns dos trabalhos, por exemplo, armazenam o documento completo na blockchain, outros passam o

documento por uma função de resumo criptográfico, armazenando apenas este resumo na blockchain. Esses dois exemplos tornam o documento publicamente verificável, porém exigem que o documento original seja exposto, a fim de ser verificado.

4. Protocolo de diploma Digital Auto-soberano com Retrocompatibilidade Tecnológica

O protocolo proposto nesta seção é baseado nas características do funcionamento do Hyperledger Indy. Primeiro, apresenta-se as definições sintáticas dos elementos utilizados na narração (§4.1). Na sequência, apresenta-se os objetos e seus tipos (§4.3). Na subseção 4.2 são apresentadas as premissas e entidades do protocolo. Por fim o 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 apresentam-se os elementos sintáticos utilizados:

Mensagem Comum - Representa uma mensagem utilizada para enviar informações entre as partes envolvidas. Uma mensagem comum do protocolo pode ser vista no Listing 1. Neste tipo de comunicação, o **emissor** envia uma mensagem para um **receptor**, ambos 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**.

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

Listing 1. Exemplo de Mensagem.

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 está no Listing 2.

```
1 IF: <Expressão>
2 DO: <Fluxo A>
3 FI:
```

Listing 2. Exemplo de Condicional.

4.2. Premissas e Entidades

A fim de se discutir na sequência a aplicabilidade e a corretude desta proposta enquanto solução, é importante se apresentar 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 2 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 as credenciais da HEI;
L	Ledger (Hyperledger Indy) - Ledger onde é publicada parte dos objetos detalhados na Tabela 3;
V	Verificador - Indivíduo que requisita uma prova e a executa, a fim de obter confirmação de uma afirmação.

Tabela 2. Entidades participantes do protocolo.

4.3. Descrição dos Objetos

Nesta subseção, apresenta-se a definição dos tipos de objetos e na sequência os objetos utilizados no protocolo. A tipagem dos objetos é determinada pela plataforma e os objetos são a instanciação destes tipos de acordo com as necessidade do protocolo. Eles são apresentado na sequência:

Definição dos Tipos de Objetos - Os objetos utilizados no protocolo são baseados naqueles utilizados pelo Hyperledger Indy e são apresentados na Tabela 3.

Objeto	Descrição
DID	Digital Identifier, é uma sequência de caracteres que identifica um usuário da rede. 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 Verynim, e é atrelado então a uma identidade pública, como uma instituição. Apenas Verynims 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 indivíduo. É mantida em posse do indivíduo e não na blockchain. Pode ser utilizada para criar Provas (Proofs) que podem ser enviadas para outros usuários e avaliadas.
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 indivíduo, de forma que essas informações não sejam conhecidas nem armazenadas por quem deseja realizar a prova.
Proof Request	Requisição criada a partir de uma Credential Schema e Credential Definition. Serve para requisitar uma prova de um indivíduo. O mesmo então a utiliza para criar a prova (Proof), que é retornada para quem a requisitou.
Verynim	DID de uma instituição ou identidade pública anteriormente registrada na Ledger.

Tabela 3. Objetos utilizados no protocolo.

Objetos - No protocolo apresentado foram criados alguns objetos próprios baseados nos tipos acima. Abreviações e descrições são apresentados na Tabela 4.

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 emitir Credenciais de diplomas.

Tabela 4. Objetos utilizados no protocolo.

4.4. Protocolo

Com base nos trabalhos relacionados analisados na seção 3 e levando em consideração as definições já apresentadas nesta seção, se propõe então um protocolo para emissão de créditos e diplomas de ensino superior de forma auto-soberana (Listing 3). Este protocolo, além de permitir grandes avanços na atual iniciativa do diploma Digital desencadeada pelo Ministério da Educação do Brasil, também trás mecanismos que permitem retrocompatibilidade tecnológica, o que permite uma migração gradual e um salto tecnológico a partir de vários pontos de partida.

É valido ressaltar que toda a comunicação entre as entidades do sistema é feita através de canais privados de comunicação. Estes canais são externos à blockchain, sendo providos por aplicações terceiras.

Devido ao uso da Hyperleger Indy, o uso da blockchain em si é restrito à publicação de DID's como Verynims, Schemas e Fefinições de Credenciais. Nenhuma credencial ou informação pessoal é armazenada na blockchain, estas informações ficam armazenadas em estruturas de dados especiais chamadas Wallets ou Carteiras, em posse física do usuário. Isto a torna uma blockchain mista, já que qualquer um com um DID pode acessar os dados porém apenas usuários com Verynims podem criar Schemas e Definições, além de emitir credenciais.

```
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 → DP Cred_Offer (DP Schema, DP Def) → S
28 S → [DP Cred_Offer] DP Cred_Request →HEI
29 HEI → [DP Cred_Request] DP → S
30 FI:
31
32 V → [DP]Proof Request → S
33 S → [Proof Request] Proof (DP) → 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
```

Listing 3. Descrição do Protocolo.

Na apresentação do protocolo, conforme o Listing 3, pode-se identificar nos primeiros passos (linhas 1 e 2) que a Autoridade Reguladora (RA) publica na Ledger (L) a definição da Credencial de Permissão de Emissão de diploma (CED). Isto permite que a RA emita estas credenciais, dando o direito as Instituições Ensino Superior (HEI) de emitir diplomas. Isto também permite que a RA revogue as credenciais que foram emitidas por ela. Na linha 4 a RA define o Schema da credencial do diploma, o que permite que na linha 6, as HEIs criem a Definição da Credencial 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. Para isso, nas linhas 14 e 15, a HEI cria o Schema e a Definição de uma Credencial de Conclusão de Disciplina (CCD). Ao final de um período letivo, para cada disciplina que o aluno completar com sucesso, nas linhas 17 a 19, a HEI oferece ao aluno uma CCD referente à disciplina concluída, via canais privados. O conjunto de credenciais que o aluno acumulado se torna o seu histórico escolar.

Após completar todas as disciplinas necessárias o aluno se qualifica para receber o diploma. Primeiramente a HEI exige que o aluno prove 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. Na linha 22, 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. Caso falte alguma CCD, o aluno não conseguirá corresponder 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, e deve 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.

Um cenário de possível utilização da Credencial do diploma é na aplicação para uma vaga de emprego, onde um aluno poderá apresentar uma prova de que possui um diploma de ensino superior. 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, através de canais privados. Ao receber a credencial o empregador pode verifica-la. Opcionalmente o Empregador/Verificador pode verificar a validade da própria instituição realizando o mesmo procedimento, ou seja, enviando a Proof Request para a HEI e recebendo a prova da validade da CED, como apresentado nas linhas 36 a 38.

Caso o Aluno possua diplomas provindos de outros sistemas legados, a retrocompatibilidade é alcançada no protocolo ao se evidenciar que o histórico escolar não é obrigatório. Para se inserir um diploma legado, é possível inserir todo o histórico escolar e realizar a prova antes de enviar o diploma completo, mas também é possível inserir um diploma sem essa prova. Para tal, é necessário encontrar formas de provar a veracidade dos outros documentos a fim de não expor vulnerabilidades para forjas e plágios. Vale ressaltar que apenas a RA teria permissão para criar o diploma desta maneira.

Ainda, é importante frisar que este modelo facilmente comporta a utilização 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, que poderiam ser credenciadas pela RA para realizar asserções sobre diplomas que já tivessem sido emitidos anteriormente.

5. Conclusões

Neste trabalho foi proposta a construção de um protocolo para a emissão e verificação de diplomas de ensino superior, utilizando a tecnologia Hyperledger Indy. Para tanto, realizou-se uma revisão sistemática da bibliografia a fim de avaliar a relevância deste tema. A partir dos resultados desta pesquisa e do funcionamento da tecnologia Hyperledger Indy, definiu-se um protocolo, levando em conta os procedimentos de emissão de diplomas atual no Brasil. [Palma et al. 2019]

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. Por sua flexibilidade, a emissão dos diplomas é uma solução 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 emissão deste documento seguindo os princípios do SSI. A origem do documento só determina o grau de automação que se pode alcançar 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.

Como trabalhos futuros, planeja-se realizar um estudo sobre a legislação Brasileira, a fim de adequar o protocolo às necessidades legais, além de garantir que este sistema estará de acordo com a Lei Geral de Proteção de Dados. Outra via de trabalho é a verificação formal do protocolo, utilizando ferramentas formais de verificação como ProVerif [Blanchet et al. 2001], o que sem dúvida determinará sua eficácia e segurança.

Referências

Abreu, A. W. S., Coutinho, E. F., and Bezerra, C. I. (2020). A blockchain-based architecture for query and registration of student degree certificates. In *SBCARS '20*, pages 151–160.

Allen, C. (2016). The path to self-sovereign identity. `http://www.lifewithalacrity.com/2016/04/the-path-to-self\-sovereign-identity.html`.

Arenas, R. and Fernandez, P. (2018). Credenceledger: A permissioned blockchain for verifiable academic credentials. In *ICE/ITMC*, pages 1–6. IEEE.

Asiri, L. (2020). *Blockchain For Educational Certificate Distribution*. PhD thesis, Florida Institute of Technology.

Ataşen, K. and Aslan, B. (2020). A blockchain based digital certification platform: Certidapp. *(JMEST*.

Averin, A., Snegireva, D., and Ladejshchikov, A. (2020). Model of a monitoring system for academic performance and the issuance of diplomas using blockchain technology. In *IT&QM&IS*, pages 88–91. IEEE.

Bahrami, M., Movahedian, A., and Deldari, A. (2020). A comprehensive blockchain-based solution for academic certificates management using smart contracts. In *2020 10th ICCKE*, pages 573–578. IEEE.

Bhumichitr, K. and Channarukul, S. (2020). Acachain: Academic credential attestation system using blockchain. In *IAIT2020*, pages 1–8.

Blanchet, B., Smyth, B., Cheval, V., and Sylvestre, M. (2001). Proverif: Automatic cryptographic protocol verifier. `https://prosecco.gforge.inria.fr/personal/bblanche/proverif/`.

Brunner, C., Knirsch, F., and Engel, D. (2019). Sproof: A platform for issuing and verifying documents in a public blockchain. In *ICISSP*, pages 15–25.

Budhiraja, S. and Rani, R. (2019). Tudocchain-securing academic certificate digitally on blockchain. In *ICICIT*, pages 150–160. Springer.

Castro, R. Q. and Au-Yong-Oliveira, M. (2021). Blockchain and higher education diplomas. *European Journal of Investigation in Health, Psychology and Education*, 11(1):154–167.

Čeke, D. and Kunosić, S. (2020). Smart contracts as a diploma anti-forgery system in higher education-a pilot project. In *MIPRO*, pages 1662–1667. IEEE.

Cheng, H. e. a. (2020). A permissioned blockchain-based platform for education certificate verification. In *BlockSys*, pages 456–471. Springer.

Dima, G.-A., Jitariu, A.-G., Pisa, C., and Bianchi, G. (2018). Scholarium: Supporting identity claims through a permissioned blockchain. In *RTSI*, pages 1–6. IEEE.

Durant, E. and Trachy, A. (2017). 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.

Fortnow, L. (1987). The complexity of perfect zero-knowledge. In *STOC '87*, pages 204–209, New York, New York.

Ghazali, O. and Saleh, O. S. (2018). A graduation certificate verification model via utilization of the blockchain technology. *JTEC*, 10(3-2):29–34.

Han, M. e. a. (2018). A novel blockchain-based education records verification solution. In *SIGITE '18*, pages 178–183.

Kaltyshev, M. (2018). *Proof of university certificate using blockchain technology*. PhD thesis, Häme University of Applied Sciences.

Leka, E. and Selimi, B. (2020). Bcert–a decentralized academic certificate system distribution using blockchain technology. *International Journal on Information Technologies & Security*, 12(4).

Lepiane, C. D., Pereira, F. L., Pieri, G., Martins, D., Martina, J. E., and Rabelo, M. L. (2019). Digital degree certificates for higher education in brazil: A technical policy specification. In *DocEng '19*, pages 1–10.

Liu, D. and Guo, X. (2019). Blockchain based storage and verification scheme of credible degree certificate. In *IICSPI*, pages 350–352. IEEE.

Liu, Y. e. a. (2020). Blockchain-based identity management systems: A review. *Journal of network and computer applications*, 166:102731.

López, M. A. (2020). Self-sovereign identity: The future of identity: Self-sovereignity, digital wallets, and blockchain. `https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignity\-digital-wallets-and-blockchain`.

Merkle, R. C. (1982). Method of providing digital signatures. US Patent 4,309,569.

Morisio, M., Ardito, L., and Yokubov, B. (2018). *Blockchain based storage of students career*. PhD thesis, Politecnico di Torino.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`.

Nguyen, D.-H., Nguyen-Duc, D.-N., Huynh-Tuong, N., and Pham, H.-A. (2018). Cvss: a blockchainized certificate verifying support system. In *SoICT 2018*, pages 436–442.

Palma, L. M., Vigil, M. A., Pereira, F. L., and Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in brazil. *International Journal of Network Management*, 29(3):e2061.

Palma, L. M. d. et al. (2020). Blockchain-based academic record system.

Patel, D. e. a. (2020). Issuing and verifying university certificates on blockchain. In *IC-BCT 2019*, pages 79–91. Springer.

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

Petre, L.-C., Paque, B., and Lejeune, C. (2019). *What are the potential benefits of blockchain applications for the Université Catholique de Louvain?* PhD thesis, Louvain School of Management.

Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing.

Raval, S. (2016). *Decentralized applications: harnessing Bitcoin's blockchain technology*. "O'Reilly Media, Inc.".

Globo G1 CE (2021). Alunos pagavam até r$ 3 mil por diploma falso emitido por faculdade no ceará. https://g1.globo.com/ce/ceara/noticia/2021/05/11/alunos-pagavam-ate-r-3-mil-por-diploma-falso\-emitido-por-faculdade-no-ceara.ghtml.

Governo Brasileiro (2001). Provisoria no 2.200-2, de 24 de agosto de 2001. http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm.

Hypeledger Foundation (2015). Hyperledger. https://www.hyperledger.org/.

Hyperledger Foundation (2018). Hyperledger indy. https://www.hyperledger.org/use/hyperledger-indy.

Ministério da Educação Brasileiro (2018). Diploma digital. http://portal.mec.gov.br/diplomadigital/#sobre.

MIT Media Labs (2016). Blockcerts-an open infrastructure for academic credentials on the blockchain. https://www.blockcerts.org/about.html.

The Sovrin Foundation (2018). Sovrin. https://sovrin.org/.

San, A. M., Chotikakamthorn, N., and Sathitwiriyawong, C. (2019). Blockchain-based learning credential verification system with recipient privacy control. In *TALE*, pages 1–5. IEEE.

Sayed, R. H. (2019). *Potential of blockchain technology to solve fake diploma problem*. PhD thesis, University of Jyväskylä.

Schär, F. and Mösli, F. (2019). Blockchain diplomas: Using smart contracts to secure academic credentials. *Journal of Higher Education Research*, 41(3):48–58.

Tokarnia, M. (2014). Ex-alunos da gama filho e univercidade têm dificuldade em obter diploma. https://agenciabrasil.ebc.com.br/educacao/noticia/2014-10/ex-alunos-da-gama-filho-e-univercidade-tem-dificuldade-\\em-obter-o-diploma.

Vidal, F. R., Gouveia, F., and Soares, C. (2020a). Blockchain application in higher education diploma management and results analysis. *ASTES*.

Vidal, F. R., Gouveia, F., and Soares, C. (2020b). Revocation mechanisms for academic certificates stored on a blockchain. In *2020 15th CISTI*, pages 1–6. IEEE.

Wood, G. et al. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32.

Yeh, L.-Y. e. a. (2018). E-university applications: A privacy-preserving diploma notarization platform in taiwan. In *EEE*, pages 44–50.