PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

PUC-SP

Daniel Márcio de Medeiros

Mecanismo de consenso em uma rede ponto a ponto distribuída para validação e registros de diplomas universitários

Mestrado em Tecnologias da Inteligência e Design Digital

São Paulo
2019

Daniel Márcio de Medeiros

Mecanismo de consenso em uma rede ponto a ponto distribuída para validação e registros de diplomas universitários

Mestrado em Tecnologias da Inteligência e Design Digital

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de MESTRE em Tecnologias da Inteligência e Design Digital – área de concentração em Processos Cognitivos e Ambientes Digitais, sob orientação do professor Dr. Demi Getschko

São Paulo
2019

FOLHA DE APROVAÇÃO

Banca Examinadora

_____

_____

_____

DEDICATÓRIA

À Deus, primeiramente,

À minha esposa Dayane, e

Aos meus pais.

AGRADECIMENTO ALUNO BOLSISTA

O presente trabalho foi realizado com o apoio da Fundação São Paulo (FUNDASP) e a Pontifícia Universidade Católica de São Paulo (PUC-SP), através da bolsa concedida, que foi de fundamental importância na realização deste trabalho.

AGRADECIMENTO

Ao meu orientador Prof. Dr. Demi Getschko pela orientação com valiosas contribuições inovadoras, pela confiança e apoio durante todo o desenvolvimento do trabalho.

Aos Profs. Dr. Daniel Gatti e Dr. Diogo Cortiz pelas preciosas contribuições durante a qualificação, tornando esse trabalho mais completo.

Ao Prof. Dr. Ítalo Vega por suas discussões científicas no decorrer das aulas, que ampliaram as possibilidades de conteúdo para este trabalho.

Ao Dr. Pe. Rodolpho Perazzolo pelo aceite de prorrogação da bolsa, graças a ele esse projeto pode ser concluído.

À minha querida esposa Dayane pelo incentivo constante mesmo nos momentos mais difíceis, pela paciência, atenção e carinho.

À minha família amada, meus pais Maurino e Vera e aos meus irmãos Danilo e Marcelo e à minha avó Lindalva, pelo carinho, paciência e apoio emocional.

À Vera Braz pelo auxílio e resolução de dúvidas, sempre disposta a ajudar.

À Edna Conti pela atenção, disponibilidade e ajuda durante todo o período.

À equipe da Compasso Tecnologia, pela compreensão e apoio durante a condução deste trabalho.

À minha querida Maya pela companhia constante durante todo o período de elaboração da dissertação.

“*O que sabemos é uma gota;*
o que ignoramos é um oceano.
Mas o que seria o oceano
se não infinitas gotas?”
Isaac Newton

RESUMO

A forma como as Instituições de Ensino Superior (IES) emitem, registram e gerenciam as credenciais acadêmicas ainda é um processo manual, burocrático e suscetível a erros e fraudes. Fraudes em diplomas acadêmicos é um problema mundial, no Brasil, por exemplo, em um único caso foram registrados 65 mil diplomas ilegais. No âmbito do sistema federal de ensino brasileiro, 84% das IES ativas não possuem prerrogativa para registrarem os diplomas de seus cursos superiores, desta forma, estas IES contratam o serviço de uma IES universitária. Neste contexto, podem ocorrer acordos ilegais e abuso de poder, fazendo-se necessário uma reorganização e padronização do processo de emissão, validação e registros de diplomas. Este trabalho analisou como as IES poderiam ser organizar para formar uma rede ponto a ponto colaborativa de emissão e registro de diplomas, respeitando a legislação vigente. Para isso, definimos uma taxonomia de termos de fraudes de diplomas, analisamos a legislação vigente, revisamos a literatura técnica do MEC quanto a fraudes de diplomas, e também a literatura sobre o uso de *blockchain* aplicados a esta problemática, e por fim, propomos um modelo conceitual de um mecanismo de consenso, definindo os requisitos, características e suas funcionalidades específicas para a emissão, validação e registro de diplomas acadêmicos. A taxonomia proposta nos indica quatro principais tipos de fraudes de diplomas no Brasil, e observamos que a legislação vigente não é capaz de combater a todas elas. Ao analisarmos o uso do *blockchain* para emissão e registro de diplomas, concluímos que esta tecnologia é muito ampla e que nem todos os tipos de *blockchain* são adequados para esta finalidade, sendo necessário a utilização de mecanismos de consenso específicos para a realidade do nosso sistema federal de ensino que garantam vantagens competitivas para as IES participantes.

Palavras-chave: Fraudes de diplomas, *Blockchain*, Mecanismo de consenso, Certificação digital, Ensino superior.

ABSTRACT

The way Higher Education Institutions (HEIs) issues, records and manage academic credentials is still a manual, bureaucratic process that is susceptible to errors and fraud. Fraud in university degrees is a worldwide problem. In Brazil, for example, in a single case 65,000 illegal degrees were registered. Under the Brazilian federal education system, 84% of active HEIs do not have the prerogative to register their higher education diplomas, so these HEIs contract the service of a university HEI. In this context, illegal settlements and abuse of power can occur, requiring reorganization and standardization of the process of issuing, validating and registering diplomas. This dissertation analyzed how to organize HEIs to form a collaborative peer-to-peer network for the issuance and registration of diplomas, in compliance with the current legislation. For this, we defined a taxonomy of terms of diploma fraud, we analyzed the current legislation, and we reviewed the MEC technical literature for diploma fraud, as well as the literature on the use of blockchain applied to this problem. Finally, we proposed a conceptual model of a consensus mechanism, defining the requirements, characteristics, and their specific functionalities for the issuance, validation and degree registration. The proposed taxonomy pointed us to four main types of university degree fraud in Brazil, and we noted that the current legislation is not capable of combating them all. By analyzing the use of blockchain for the issuance and registration of diplomas, we concluded that this technology is very broad and that not all blockchain types are suitable for this purpose and it is necessary to use consensus mechanisms specific to the reality of our federal system. Teaching that will guarantee competitive advantages to the participating HEIs.

Key Words: University degree fraud, Blockchain, Consensus mechanism, Digital certification, Higher education.

Sumário

1 INTRODUÇÃO 14

1.1 CLASSIFICAÇÃO DE IES POR FUNÇÃO DE REGISTRO E EXPEDIÇÃO DE DIPLOMAS 15

1.2 EXPEDIÇÃO E REGISTRO DE DIPLOMAS DE CURSOS SUPERIORES NO BRASIL 17

1.3 PROCESSO TÍPICO DE REGISTRO DE DIPLOMAS 19

1.4 LEI DA INFORMAÇÃO E DADOS ABERTOS NO BRASIL 20

1.5 LEI DE PROTEÇÃO DE DADOS E IDENTIDADE DIGITAL 21

1.6 TIPOS DE CRIMES DA INFORMAÇÃO SEGUNDO CÓDIGO PENAL BRASILEIRO 23

1.7 VAZAMENTO DE DADOS E PRIVACIDADE SEGUNDO A LGPD 24

1.8 TIPOS DE ARQUIVAMENTO DE DOCUMENTOS 24

1.9 OBJETIVOS 25

1.9.1 Objetivo Geral 25

1.9.2 Objetivos Específicos 25

1.10 METODOLOGIA 26

1.11 TAXONOMIA PROPOSTA 27

1.12 PORTARIAS DO MEC PARA O COMBATE À FRAUDE DE DIPLOMAS 28

1.13 USO DE DIPLOMAS DIGITAIS 30

1.13.1 Vantagens do diploma digital 31

1.13.2 Desvantagens do diploma digital 32

2 DESAFIOS NO SERVIÇO DE EMISSÃO E VALIDAÇÃO DE DIPLOMAS 33

2.1 LIMITAÇÕES DO MODELO ATUAL PROPOSTO PELAS PORTARIAS VIGENTES 33

2.2 DESAFIO NO COMBATE DE FRAUDE DE DIPLOMA EXTRALEGAL 34

2.3 DESAFIO NO USO DO DIPLOMA DIGITAL 35

2.4 PRESERVAÇÃO DIGITAL 36

***3 BLOCKCHAIN* 37**

3.1 CAMADAS DO *BLOCKCHAIN* 38

3.1.1 Rede Peer-to-Peer (P2P) 39

3.1.2 Mecanismo de Consenso 39

3.1.3 Propagação na transação na rede distribuída 40

3.1.4 Prova criptográfica 40

3.1.5 Aplicação 40

3.2 PROPRIEDADES DO *BLOCKCHAIN* 41

3.3 FUNÇÃO *HASH* 41

3.4 ESTRUTURA DE DADOS 41

3.5 ÁRVORE MERKLE 42
3.6 LEDGER 43
4 ESTADO DA ARTE 44
5 A PESQUISA 47
6 MODELO DE MECANISMO DE CONSENSO 49
6.1 REDES COLABORATIVAS 49
6.2 REQUISITOS DO MECANISMO DE CONSENSO 50
6.3 REGRAS DO MECANISMO DE CONSENSO DO LIVRO DE REGISTRO DISTRIBUÍDO 51
6.3.1 Definição de bloco e lote de diplomas 52
6.3.2 Estrutura de dados do lote de diplomas 52
6.3.3 Descrição da fila de lotes de diplomas a serem registrados 53
6.3.4 Critérios de seleção e classificação da IES líder 54
6.3.5 Descrição da fila de IES registradoras 57
6.3.6 Incentivos do mecanismo de consenso 58
6.4 BENEFÍCIOS PARA A SOCIEDADE E O SISTEMA DE ENSINO 59
7 DISCUSSÃO 60
7.1 LIMITAÇÕES 63
7.2 TRABALHOS FUTUROS 63
7.3 CONCLUSÃO 64
8 REFERÊNCIAS 65

ÍNDICE DE ILUSTRAÇÕES

Figura 1 – Blocos encadeados no *blockchain* 38
Figura 2 – Decomposição por camadas da tecnologia *blockchain*.....38
Figura 3 – Representação visual da árvore Merkle 42
Figura 4 – Taxa média paga por transação no blockchain do Bitcoin e do Ethereum. período de um ano.....45
Figura 5 – Mecanismo de consenso para a escolha da IES registradora líder.....53
Figura 6 – Processo de replicação dos novos registros de diplomas entre as IES participantes.....58

ÍNDICE DE TABELAS

Tabela 1 – Grupos de IES segmentadas por atribuição de registro de diplomas.....15
Tabela 2 – Quantidade de IES por grupo e por unidade federativa.....17
Tabela 3 – Valor cobrado para registro de diploma 19
Tabela 4 – Categorias de fraudes de diplomas.....27
Tabela 5 – Exemplos de características de diplomas irregulares por tipo de fraudes de diplomas.....28
Tabela 6 – Características de segurança da informação de um diploma digital.....31
Tabela 7 – Tipos de fraudes resolvidas por dispositivos legais vigentes.....34
Tabela 8 – Tipos de *blockchain* segmentados por modelo de permissão.....37
Tabela 9 – Parâmetros que compõe a nota do serviço prestado pela IES registradora a cada lote de diplomas.....56

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

AWS - Amazon Web Services

CNE - Conselho Nacional de Educação

DLT - *Distributed Ledger Technology*

DOU - Diário Oficial da União

e-MEC - Portal do MEC

EAD - Ensino a Distância

GED - Gestão Eletrônica de Documentos

ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira

IES - Instituições de Ensino Superior

INEP - Instituto Nacional de Estudos e Pesquisas Educacionais

IoT - *Internet of Things*

IPA - Interface de Programação de Aplicativos

Ledger - livro de registros

LGPD - Lei Geral de Proteção de Dados

MEC - Ministério da Educação

MIT MEDIA LAB - *Research Laboratory at the* MIT

MIT - Massachusetts Institute of Technology

NBR - Normas Brasileiras

P2P - Rede ponto a ponto

PBAD - Padrão Brasileiro de Assinatura Digital

PGB - Problema dos Generais Bizantinos

PoR - *Proof of Reputation*

SHA-256 - *Secure Hashing Algorithm*

TSA - *Authority Timestamp*

UFBA - Universidade federal da Bahia

UFES - Universidade federal do Espírito Santo

UFG - Universidade federal de Goiás

UTXO - *Unspent Transaction Output*

XAdES - *Advanced Electronic Signature*

XML - *Extensible Markup Language*

1 Introdução

A tecnologia digital vem transformando a educação brasileira ao possibilitar novos caminhos de aprendizagem personalizados, como por exemplo, com o desenvolvimento e disseminação do ensino à distância (EAD). Além disso, a informatização de sistemas de gestão acadêmicas tornam acessíveis o histórico acadêmico do aluno até a conclusão do curso. Entretanto, a forma como as Instituições de Ensino Superior (IES) emitem e gerenciam as credenciais acadêmicas ainda é um processo manual, burocrático e suscetível a erros e fraudes.

Fraudes em diplomas acadêmicos é um problema mundial. No Brasil, por exemplo, em um caso emblemático a IES UNIG, que conforme relato público de um processo administrativo instaurado pelo Ministério da Educação (MEC) em 2018, registrou mais de 65.000 diplomas ilegais. Atualmente muitos países estão interessados em resolver esse problema com o uso de tecnologias como *blockchain* e assinatura digital, entre eles, Austrália, Reino Unido e Estados Unidos estão à frente desse processo (Jirgensons e Kapenieks, 2018).

Usar diplomas falsos não é uma atividade sem vítimas. Empresas e instituições podem contratar pessoas sem a qualificação necessária e obrigatória, oferecendo serviços em condições inadequadas ao público em geral, o que torna um problema social. Além disso, fraudes de diplomas podem desvalorizar e diminuir a reputação das IES em situação regular (Grolleau, Lakhal e Mzoughi, 2016).

O MEC, desde 2016, através das portarias normativas revogadas N° 7 e 8, sinalizou a urgência e importância de criar um arcabouço legislativo no combate a fraudes, irregularidades e a crescente expansão do mercado ilegal de vendas de diplomas acadêmicos. A proposta era a criação de um Cadastro Nacional dos Concluintes de cursos superiores. O INEP (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira) teria a responsabilidade em estruturar e disponibilizar o Cadastro de Diplomas do MEC. Como a portaria não especificava os detalhamentos da criação do cadastro, a mesma foi revogada por deficiência de critérios técnicos. Essa iniciativa do governo federal revelou dificuldades no sistema de fiscalização, controle social, e na validação das informações do diploma (Portal MEC, 2016).

Após a descontinuação das portarias anteriores, foi publicada em 25 de outubro de 2018 a portaria N° 1.095, que transferiu e atribuiu a responsabilidade da validação das informações acadêmicas para as IES públicas e privadas. Esta portaria traz um

grande avanço no combate a diplomas irregulares. Trata-se de um passo importante na direção de dificultar fraudes e irregularidades. No entanto, esta portaria é uma etapa inicial no controle social e fiscalizatório de verificação das informações de um diploma.

1.1 Classificação de IES por função de registro e expedição de diplomas

O MEC regulamenta que as IES, pertencentes ao sistema federal de ensino, são responsáveis pela emissão e validação dos diplomas de seus cursos de graduação e pós-graduação. A emissão e registro de diplomas são regulamentados pelo MEC através de diversas portarias, sendo que a portaria N° 1.095/18 consolidou o modelo de emissão e registro de diplomas e adicionou alterações a esse modelo. Dentre as alterações, houve um importante passo para a utilização de tecnologia da informação no processo de expedição de diplomas.

O sistema federativo brasileiro é composto por instituições públicas e privadas com três níveis de autonomia de registros de diplomas. As IES podem ser agrupadas, conforme a tabela abaixo:

Tabela 1 – Grupos de IES segmentadas por atribuição de registro de diplomas.

Grupo 1	IES que podem expedir e registrar seus diplomas e registrar diplomas de outras IES não universitárias: Universidades, os Institutos Federais de Educação, Ciência e Tecnologia e os Centros Federais de Educação Tecnológica.
Grupo 2	IES que só podem expedir e registrar seus próprios diplomas: Centros Universitários, Faculdades vinculadas ao sistema Federal de ensino que receberam atribuição de registrar seus próprios diplomas.
Grupo 3	IES que expedem, mas não podem registrar seus diplomas: IES não universitárias (IES isolada).

Art. 1° da resolução CNE/CES N° 12 de 2017 regulamenta que:

> “Os diplomas dos cursos de graduação e sequenciais de formação específica expedidos por instituições não-universitárias serão registrados por universidades credenciadas, independentemente de autorização prévia deste Conselho.”

Ou seja, as IES do grupo 1 (universitárias), que podem registrar os diplomas de outras IES oferecem esse serviço por delegação do MEC, e esse serviço é cobrado. Antes desta resolução, o MEC determinava para cada IES isolada respectivamente as IES registradoras. Após a resolução N° 12/13 de 2017, as IES isoladas passaram a escolher livremente as IES registradoras. Desta forma, o MEC regulamentou a oferta de IES registradoras capazes de atenderem a demanda das IES expedidoras no Brasil. No Sistema Federativo Brasileiro, segundo o último levantamento publicado no portal e-MEC existem 3073 IES ativas, segmentadas de acordo com os três grupos de IES (Tabela 2).

A tabela a seguir apresenta os números de IES ativas. Atualmente, segundo o portal e-MEC, já foram extintas mais de 249 IES. Dentre as IES ativas, a maioria são faculdades (IES isoladas), e este grupo representa 84% das IES no Brasil. Isso significa que grande parte do registro de diplomas é realizado por uma IES diferente da qual o expediu. Segundo o Censo da Educação Superior, fornecido pelo INEP em 2017, houve um total de 1,2 milhões de concluintes, e por consequência, 1,2 milhões de diplomas expedidos.

Tabela 2 - Quantidade de IES por grupo e por unidade federativa.

IES do Estado Federativo Brasileiro divididas por grupo				
Unidade Federativa	Universidade	Centro Universitário	Faculdade	Total
AC	1	3	10	**14**
AL	3	4	29	**36**
AM	3	5	19	**27**
AP	2	1	13	**16**
BA	10	15	147	**172**
CE	7	12	83	**102**
DF	2	10	70	**82**
ES	2	5	87	**94**
GO	4	9	107	**120**
MA	5	3	53	**61**
MG	22	31	325	**378**
MS	5	3	40	**48**
MT	3	4	65	**72**
PA	6	6	59	**71**
PB	3	4	46	**53**
PE	5	12	121	**138**
PI	2	3	45	**50**
PR	15	24	205	**244**
RJ	17	23	114	**154**
RN	4	3	25	**32**
RO	1	3	35	**39**
RR	2	2	4	**8**
RS	21	10	113	**144**
SC	13	16	94	**123**
SE	2	1	20	**23**
SP	38	81	612	**731**
TO	3	3	35	**41**
Total de IES	**201**	**296**	**2576**	**3073**

1.2 Expedição e registro de diplomas de cursos superiores no Brasil

No Brasil, a validade jurídica de um diploma em todo território nacional é alcançada no ato de transcrição do diploma para o livro de registro de uma IES registradora. AS IES registradoras exercem uma função social de validadoras e guardiãs das informações dos diplomados no Brasil. Ao contrário do que o senso comum acredita, o MEC não registra e também não possui uma base de dados de diplomas.

A portaria N° 1.095/18 consolidou um modelo de emissão e registro de diplomas e ainda estabeleceu novas regras. Conforme o Art. 14 desta portaria, um

registro típico deverá conter obrigatoriamente pelo menos as informações que estão listadas abaixo:

I – número de registro;

II – número do diploma;

III – número do processo;

IV – nome completo do diplomado;

V – data e local de nascimento;

VI – nacionalidade;

VII – cédula de identidade, indicando o órgão expedidor e a Unidade da Federação;

VIII – nome do curso;

IX – atos de autorização, de reconhecimento ou de renovação de reconhecimento do curso com a data de publicação no DOU;

X – data da conclusão do curso;

XI – data da colação de grau;

XII – data da expedição do diploma;

XIII – data do registro do diploma;

XIV – título ou grau conferido;

XV – nome da instituição de educação superior;

XVI – razão social da mantenedora da instituição de educação superior e respectivo número do Cadastro Nacional de Pessoas Jurídicas – CNPJ;

XVII – nome e número do CPF do responsável pelo registro ou, no caso de servidor público, o número da matrícula;

XVIII – assinatura do dirigente máximo ou do responsável formalmente designado, com a indicação do ato de delegação respectivo.

Todos os diplomas são registrados em livros físicos, com um termo de abertura e registro de anotações e expedições dos documentos. Além da forma física, o livro de registro pode ser também digital a partir da Portaria N° 554/19. Neste segundo caso, é necessário que a assinatura digital do registro atenda os requisitos da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira).

Segundo Aparecida e Barbosa (2010), transcrição em livro de registro físico é algo manual e suscetível a erros, podendo ocorrer o preenchimento de dados incompletos e muitas vezes não há nenhuma ação para tratar essa problemática.

As IES universitárias conforme descrito na sessão 1.1 podem ofertar esse serviço de forma independente para as IES isoladas. Os valores cobrados, em média são da ordem de R$80,00 por diploma registrado (Tabela 3). Segundo a legislação atual cada IES registradora tem autonomia para estruturar, organizar e gerir uma unidade registradora na Universidade.

Tabela 3 -Valor cobrado para registro de diploma de graduação (dados extraídos no site das IES na data de 25/02/2019).

Universidade Registradora	Valor cobrado registro de diploma de graduação
UFSCAR	R$ 100,00
UFMG	R$ 30,00
USP	R$ 150,00
UNICAMP	R$ 180,00

As IES expedidoras também escolhem livremente as IES registradoras, e o processo de registro ocorre como uma prestação de serviços. Não há uma padronização nesse tipo de serviço. O nível de exigência e qualidade das informações requeridas para instrução do processo de registros de diploma fica a cargo da IES registradora.

1.3 Processo típico de registro de diplomas

As IES com prerrogativas para o registro de diplomas possuem autonomia para definirem o seu próprio fluxo no processo de registro. Esta condição na legislação em vigor ressalta a autonomia universitária, mas ao mesmo tempo não oferece para as IES uma referência técnica de boas práticas no processo de registro de diplomas.

Essa situação é constatada ao comparar os manuais de registro de diplomas oferecidos pelas unidades registradoras das IES universitárias. Com base na análise de 3 manuais de diferentes IES universitárias UFBA, UFES e UFG, vimos que não há uma padronização no processo de registro, cada unidade registradora pode solicitar

informações diferentes, em diferentes formatos, com diferentes formas de comprovação de documentos.

Vimos que a UFBA, por exemplo, solicita uma cópia simples do certificado de conclusão do ensino médio e histórico escolar da graduação, por sua vez a UFES solicita uma cópia autenticada ou a original do certificado de conclusão do ensino médio acompanhado do respectivo histórico escolar original, já a UFG solicita a cópia autenticada do certificado de conclusão do ensino médio acompanhado do respectivo histórico escolar e uma cópia simples do histórico escolar da graduação (UFBA, 2014; UFES, 2016; UFG, 2011).

A prática observada na leitura desses manuais de solicitação de cópias autenticadas de documentos ou mesmo cópias simples tem sua eficácia muito questionável como comprovação, pois a autenticidade em cartório não confere necessariamente a veracidade do documento.

Apesar de não identificarmos um padrão nesse processo, nossa análise permitiu identificarmos um fluxo mínimo comum. A seguir, um exemplo resumido de um processo típico de registro de diplomas entre IES isolada e IES universitária:

1. Solicitação de registro de diploma pela IES isolada.
2. Encaminhamento da documentação da IES isolada exigida no processo (Art. 12° da portaria N° 1.095/18).
3. Encaminhamento da documentação do diplomado.
4. Análise da documentação exigida do diplomado no processo.
5. Se houver necessidade, revisão ou solicitação de documentação complementar.

As IES do Grupo 2 (centros universitários) não realizam esse processo, pois emitem e registram seus próprios diplomas, assim como, as IES universitárias em relação aos diplomas emitidos por suas próprias faculdades.

1.4 Lei da Informação e dados abertos no Brasil

A Lei N° 12.527/2011 regulamenta o direito constitucional de obter informações públicas. Essa norma entrou em vigor em 16 de maio de 2012 e criou mecanismos que possibilitam a qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades.

Considerando essa lei, podemos destacar oito princípios de dados abertos governamentais definidos pelo *Open Government Data* (Malamud, 2007):

- Completos: Dados públicos são dados que não estão sujeitos a limitações válidas de privacidade, segurança ou controle de acesso, reguladas por estatutos;
- Primários: os dados são apresentados tais como os coletados na fonte, com o maior nível possível de granularidade e sem agregação ou modificação;
- Atuais: os dados são disponibilizados o quão rapidamente seja necessário para preservar o seu valor;
- Acessíveis: os dados são disponibilizados para o público mais amplo possível e para os propósitos mais variados possíveis;
- Processáveis por máquina: os dados são razoavelmente estruturados para possibilitar o seu processamento automatizado;
- Acesso não discriminatório: os dados estão disponíveis a todos, sem que seja necessária identificação ou registro;
- Formatos não proprietários: os dados estão disponíveis em um formato sobre o qual nenhum ente detenha controle exclusivo;
- Livres de licenças: os dados não estão sujeitos a regulamentação de direitos autorais, marcas, patentes ou segredo industrial. Restrições razoáveis de privacidade, segurança e controle de acesso podem ser permitidas na forma regulada por estatutos.

A abertura de dados promove transparência e, ao mesmo tempo, estimula o engajamento popular, ao aumentar a disponibilidade de informações atualizadas e de qualidade e por esse motivo, a ação de abertura de dados governamentais possui impacto direto na melhoria da gestão pública e estímulo ao controle social.

1.5 Lei de proteção de dados e Identidade digital

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei Nº 13.709/2018, é a legislação brasileira que regulamenta as atividades de tratamento de dados pessoais e disciplina como estes dados devem ser armazenados por empresas ou mesmo por outras pessoas físicas.

Essa lei regulamenta que organizações públicas e/ou privadas só poderão coletar dados pessoais se tiverem consentimento do usuário de seus sistemas ou de seus clientes. O titular dos dados deverá ser informado sobre o que exatamente será coletado, para quais fins os dados serão utilizados e se haverá compartilhamento. Além da obrigatoriedade da formalização do consentimento por parte do titular, este poderá, sempre que desejar, revogar a sua autorização, bem como pedir acesso, exclusão, portabilidade, complementação ou correção de seus dados.

Para as IES públicas e privadas as adequações realizadas para o cumprimento da Portaria Nº 1095/18 em manter e disponibilizar um banco de informações de registro de diplomas de seus cursos superiores para consulta pública devem obrigatoriamente está em conformidade com as regras da LGPD. Desta forma, as IES deverão incluir mecanismos em seus procedimentos internos, que capturem a expressa formalização e consentimento do seu aluno de quais dados serão divulgados na internet. A mesma condição se aplica também para o diploma digital, regulamentado pela Portaria Nº 554/19, que entrará em vigor a partir de 2021.

Embora a LGPD tenha como proposta melhorar a transparência da finalidade e tratamento do uso de dados de terceiros, a aplicação desta lei ainda é um desafio para a correta utilidade de algumas tecnologias, como por exemplo o *blockchain*, que impossibilita a exclusão de registros de dados e os armazenam de forma imutável. No entanto, a imutabilidade no armazenamento dos dados no *blockchain* não impossibilita o cumprimento da LGPD, uma vez que os dados armazenados poderão ser simplesmente o *hash* de uma determinada informação primária, ou mesmo dependendo do protocolo de consenso o acesso ao dado, com o uso de chaves criptográficas poderá ser revogado e a visualização dos dados controlada pelo seu titular. Segundo Ventura (2019) a LGPD proporciona 9 direitos aos titulares de dados no Brasil:

- Confirmação e Acesso aos Dados: o titular dos dados tem o direito de confirmação da existência de tratamento dos mesmos e, por consequência, acessar todos os seus dados pessoais que foram coletados e tratados pelo controlador.
- Retificação: o titular dos dados tem o direito de corrigir dados incompletos, inexatos ou desatualizados.

- Restrição de tratamento: o titular dos dados tem o direito de restringir o tratamento de dados pessoais, por meio da recusa em fornecer o consentimento.
- Cancelamento ou exclusão: o titular dos dados tem o direito de pedir o cancelamento ou exclusão de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
- Portabilidade: o titular dos dados tem o direito de transferir os seus dados pessoais de um controlador para outro.
- Revogação de consentimento: o titular dos dados pode revogar a autorização para o tratamento de seus dados pessoais a qualquer momento, bastando uma manifestação expressa, por procedimento gratuito e facilitado.
- Oposição: o titular dos dados tem o direito de se opor a quaisquer tratamentos e informações que não estejam em conformidade com a lei, assim como as decisões automatizadas que afetem seus interesses, como decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
- Explicação: o titular dos dados tem direito a receber informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo controlador para a tomada de decisão com base em tratamento automatizado de dados pessoais.
- Direito à informação: o titular dos dados tem o direito de receber informações sobre as entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

1.6 Tipos de crimes da informação segundo código penal brasileiro

O Código penal brasileiro (Decreto Lei 2848/40) tipifica crimes praticados no âmbito da administração pública, desta forma, diante do código penal há uma distinção entre as IES públicas e privadas na responsabilidade da segurança dos seus bancos de dados e sistemas informatizados. As IES públicas no quesito de segurança do seu conjunto de informações, inclusive no meio informatizado, devem ser modificadas somente nos limites legais. Abaixo relacionamos a tipificação dos crimes contra IES públicas.

- **Inserção de dados falsos em sistema de informações**

Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da administração pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

- **Modificação ou alteração não autorizada de sistema de informações**

Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.

- **Extravio, sonegação ou inutilização de livro ou documento**

Art. 314 - Extraviar livro oficial ou qualquer documento, de que tem a guarda em razão do cargo; sonegá-lo ou inutilizá-lo, total ou parcialmente.

1.7 Vazamento de dados e privacidade segundo a LGPD

As IES como agentes de tratamento de dados, devem adotar medidas de segurança em seus bancos de dados que tenham dados pessoais de seus alunos e funcionários. A administração e o manejo desses dados devem observar o direito à privacidade e proteção dos dados pessoais de acessos não autorizados. Segundo o Art. Nº 48 da LGPD, em caso de incidente de segurança com potencial de risco ou danos aos titulares de dados, as IES devem comunicar a autoridade nacional a respeito do incidente.

A referida comunicação, conforme exigência legal, deve ser realizada em prazo razoável e deverá conter, no mínimo, as seguintes informações: (i) natureza dos dados pessoais afetados; (ii) informações sobre os titulares envolvidos; (iii) indicação de medidas mitigadoras e de segurança utilizadas para a proteção dos dados; (iv) os riscos envolvidos no acidente; e caso a comunicação não seja imediata, (v) as razões da demora.

1.8 Tipos de arquivamento de documentos

De acordo com a Portaria N° 1095/18 as IES públicas e privadas deverão manter banco de informações de registro. Diante desta exigência é importante

apresentarmos os tipos de documentos de arquivos e seus respectivos critérios conforme a ABNT através da NBR 9578/86 e NBR 10519/88:

- Arquivo corrente – documento de caráter técnico e administrativo sujeito a consultas frequentes por parte do órgão que o constituiu.
- Arquivo intermediário – documentos de uso não frequente, originários de arquivos correntes, que devem aguardar destinação final em depósito temporário.
- Arquivo permanente – documentos de guarda definitiva em decorrência do seu valor probatório e informativo.

O banco de informações de registros regulamentado pela portaria N° 1095/18 refere-se ao tipo de arquivo permanente, sendo assim trata-se de um desafio a preservação destes arquivos nas IES. O uso do *blockchain* poderá possibilitar uma guarda compartilhada e permanente entre as IES, diminuindo desta forma, o risco de um eventual incidente ou extravio dos dados.

1.9 Objetivos

O objetivo principal do nosso trabalho é propor um modelo conceitual de um mecanismo de consenso de validação confiável e registro imutável de diplomas acadêmicos. Este modelo tem em vista a resolução de fraudes cometidas por IES emissoras e registradoras de diplomas. Iremos identificar e classificar as fraudes de diplomas acadêmicos no âmbito do sistema federal de ensino e iremos realizar uma reflexão da legislação atual no contexto abordado.

1.9.1 Objetivo Geral

Propor um modelo conceitual de um mecanismo de consenso em uma rede ponto a ponto (P2P) distribuída para validação e registro imutável de diplomas acadêmicos.

1.9.2 Objetivos Específicos

- Definir uma taxonomia de fraudes de diplomas acadêmicos.

- Analisar o arcabouço legal e identificar possíveis limitações para o combate de fraudes de diplomas.
- Avaliar a adequação do uso do *blockchain* público na validação e registro de diplomas.
- Propor um modelo conceitual de um mecanismo de consenso de validação e registro de diplomas de cursos superiores.

1.10 Metodologia

Tendo em vista a questão central da pesquisa: Como as IES do sistema federal de ensino, no âmbito da legislação vigente, podem ser organizadas em uma rede cooperativa de emissão, validação e registro de diplomas digitais para prover um serviço que diminua as fraudes discutidas nesse trabalho? E levando em consideração também os objetivos específicos desse trabalho, optamos por uma abordagem exclusivamente qualitativa que norteará os seguintes tópicos:

a) Revisar a literatura científica e normas técnicas do MEC sobre fraudes de diplomas acadêmicos no âmbito do sistema federal de ensino.
b) Sistematizar e compilar a revisão bibliográfica do item anterior e propor uma taxonomia de termos sobre fraudes de diplomas.
c) Revisar a literatura sobre *blockchain* aplicados ao processo de emissão e registro de diplomas acadêmicos.
d) Analisar as Portarias Nº 1095/18 e Nº 554/19 sobre as mudanças no processo de expedição e registros de diplomas acadêmicos.
e) Compreender os incentivos e benefícios de participação das IES do sistema federal de ensino organizadas numa rede colaborativa ponto a ponto para emissão e registro de diplomas.
f) Elaborar um modelo conceitual de um mecanismo de consenso, definindo os requisitos, características e suas funcionalidades.

O desenvolvimento das etapas elencadas acima terá como premissa uma pesquisa de natureza teórica e exploratória que resultará num corpo de conhecimento sistematizado que visa apresentar questões a serem usadas em pesquisas subsequentes, porém, não almejamos obter respostas definitivas para a nossa questão de pesquisa.

1.11 Taxonomia proposta

Atualmente há pouco estudo ou pesquisa acadêmica para viabilizar um limite semântico quando se fala em tipos de fraudes de diplomas no Brasil. Neste sentido, vamos propor uma terminologia adequada para delimitar com exatidão o que constitui cada tipo de fraude de diploma (Tabela 4).

Tabela 4 - Categorias de fraudes de diplomas.

Categoria de Diplomas inválidos	
Termo da taxonomia	Definição do termo
Diploma adulterado	São diplomas de origens oficiais e legítimas que foram adulterados por omissões, acréscimos ou alterações de informações. Exemplos de alterações: data de nascimento, ano de formação, data de colação de grau, grau conferido.
Diploma fictício	Réplica que forja a imitação visual de um diploma. Diploma criado fora dos trâmites legais de uma IES. Falsificação criada para imitar um diploma válido. Um documento fictício trata-se simplesmente de um similar em aparência a um original.
Diploma ilegítimo	Diploma expedido por uma IES isolada devidamente credenciada, mas o seu titular não tem uma trajetória acadêmica verdadeira e/ou válida. Venda de diplomas sem um lastro acadêmico. A fraude pode ser a ilicitude na expedição do diploma, seu registro não existe na IES registradora. Essa situação trata-se de uma irregularidade na expedição de diplomas de uma IES. Isso pode ocorrer com ou sem o consentimento da IES, no livro de registro físico ou digital.
Diploma extralegal	Diploma expedido por uma IES devidamente credenciada e registrado por uma IES com prerrogativas para tal, mas o seu titular não tem uma trajetória acadêmica verdadeira e/ou válida. Venda de diplomas sem um lastro acadêmico. A fraude pode ser a ilicitude no processo de registro de um diploma. A IES registradora transcreve informações incorretas ou inexistente em seu livro de registro. Essa situação trata-se de uma fraude na unidade expedidora e registradora de diplomas de uma IES.

Os tipos de fraudes descritas acima podem produzir, por exemplo, os seguintes diplomas irregulares:

Tabela 5 – Exemplos de características de diplomas irregulares por tipo de fraudes de diplomas.

Tipo de fraude	Possíveis características de diplomas irregulares e/ou ilegais
Diploma extralegal	Diploma de um curso superior credenciado de uma IES devidamente credenciada
Diploma ilegítimo	Diploma de um curso superior não credenciado de uma IES devidamente credenciada
Diploma ilegítimo	Diploma de um curso superior de uma IES descredenciada
Diploma fictício	Diploma de um curso superior de uma IES extinta
Diploma fictício	Diploma de um curso superior de uma IES inexistente
Diploma fictício	Diploma de um curso superior inexistente de uma IES existente
Diploma adulterado	Diploma de um curso superior credenciado de uma IES regular, porém, sofreu alguma adulteração das informações contidas no mesmo.

A tabela acima apresenta algumas possibilidades de fraudes de acordo com a classificação taxonômica proposta. No entanto, podem existir outras situações que podem gerar os tipos de fraudes propostos na tabela 4.

1.12 Portarias do MEC para o combate à fraude de diplomas

As normativas N° 315/18, N° 1.095/18 e N° 554/19 são um marco regulatório importante na modernização dos serviços de expedição e registro de diplomas de cursos superiores prestados pelas IES do Brasil. A implementação tecnológica dos dispositivos deste compilado regulatório será um avanço significativo, na agilidade, transparência, segurança e validação de diplomas.

A Portaria Nº 315/18 define as regras que as IES deverão adotar para a digitalização dos documentos referentes à vida acadêmica de seus estudantes para comprovar sua trajetória acadêmica, desde a matrícula até a colação de grau. A nova

regra inclui também a implementação de processo de gestão documental (GED) em todo o acervo acadêmico.

Essa portaria ao instituir a gestão documental nas IES públicas e privadas colabora com o combate de fraudes de diplomas na medida que facilita a fiscalização e o monitoramento pelos órgãos competentes além de disciplinar a transferência do acervo acadêmico de IES extintas ou em processo de extinção para uma IES pública ou privada interessada pelo acervo, ou então, caso não haja uma IES interessada, o acervo acadêmico da IES extinta ou em processo de extinção devem ser transferidos para uma IES pública, escolhida pelo MEC.

O Art. 45° da portaria N° 315/18 regulamenta que:

> “Nos termos do art. 104 do Decreto nº 9.235, de 2017, os documentos e informações que compõem o acervo acadêmico, independente da fase em que se encontrem ou de sua destinação final, conforme Código e Tabela aprovados pela Portaria AN/MJ no 92, de 2011, deverão ser convertidos para o meio digital, no prazo de vinte e quatro meses, de modo que a conversão e preservação dos documentos obedeçam aos seguintes critérios:”

A portaria N° 1.095/18 estabeleceu novas regras para a emissão e registro de diplomas. Entre elas, a necessidade de as IES tornarem públicas em seus sites os dados do aluno diplomado e informações sobre a expedição de sua diplomação. Além disso, a IES registradora deve publicar no Diário Oficial da União (DOU) a informação da quantidade de diplomas registrados da mantenedora, e informar também a URL para consulta pública dos diplomas. Desta forma, as instituições que emitem e registram são também as que devem prover publicamente mecanismos de validação.

O Art. 23° da portaria N° 1.095/18 regulamenta que:

> “As IES públicas e privadas deverão manter banco de informações de registro de diplomas a ser disponibilizado no sítio eletrônico da IES e, após realizado o devido registro, terão o prazo de trinta dias para incluir os dados para consulta.”

A portaria N° 554/19 estabeleceu a obrigatoriedade de as IES públicas e privadas implantarem a emissão e o registro dos diplomas de seus cursos de graduação por meio digital. O diploma digital passa a compor obrigatoriamente a documentação acadêmica do aluno diplomado e, além disso, o livro de registro deve existir além da forma física, na forma digital.

O Art. 2° da portaria N° 554/19 regulamenta que:

> "As IES públicas e privadas pertencentes ao Sistema Federal de Ensino deverão implementar a emissão e o registro dos diplomas de seus cursos de graduação por meio digital, nos termos desta Portaria.
> § 1º O diploma digital é aquele que tem sua existência, sua emissão e seu armazenamento inteiramente no meio digital, e cuja validade jurídica é presumida mediante a assinatura com certificação digital – ICP-Brasil ..."

Segundo dados oficiais da plataforma e-MEC, atualmente há mais de 3000 IES ativas e regulamentadas no Brasil. Segundo a portaria N° 1.095/18, a regularidade da IES e seus respectivos cursos são condições necessárias para a validade jurídica de um diploma, além da transcrição em livro de registro.

De acordo com as normativas citadas, as mudanças recentes na legislação vão promover a transformação digital nos processos de emissão, registro e guarda de dados, além de tornar públicas informações para aumentar o nível de segurança dos diplomas. Cada IES atua como uma autoridade central na emissão e validação de seus diplomas, desta forma, a mesma autoridade de emissão é também a fonte de validação pública.

1.13 Uso de diplomas digitais

Segundo a portaria N° 554/19, o diploma digital tem sua origem, emissão, registro e armazenamento em ambiente digital e tem a mesma validade jurídica do documento impresso. A validade do documento é garantida por assinatura com certificação digital e carimbo de tempo na ICP-Brasil, conforme os parâmetros do Padrão Brasileiro de Assinaturas Digitais.

A assinatura do diploma com certificação digital na ICP-Brasil, atribui as seguintes características de segurança ao documento (Queiroz, 2014), conforme tabela abaixo:

Tabela 6 - Características de segurança da informação de um diploma digital.

Serviço de	Descrição
Autenticidade	O receptor pode confirmar a assinatura feita pelo emissor
Irretratabilidade	O emissor não pode negar a autoria da assinatura
Integridade	O receptor tem a garantia que o documento não foi adulterado

A portaria N° 554/19 regulamenta que o diploma digital deve ser emitido no formato XML, valendo da assinatura avançada no padrão XML – XadES. É facultativo a representação visual do diploma digital, desde que se observe a exatidão e fidedignidade das informações prestadas no XML.

A emissão e o registro do diploma digital estão inclusos nos serviços educacionais prestados pelas IES e o mesmo integra os documentos institucionais como parte de seu acervo acadêmico.

A certificação digital ICP-Brasil garante as seguintes propriedades aos diplomas digitais: autenticidade, integridade, confiabilidade e o não-repúdio. O certificado tem validade por tempo determinado e pode ser revogado pela autoridade certificadora. O certificado no âmbito do ICP-Brasil por si só não garante a regularidade da IES, pois a condição legal para sua obtenção é a situação cadastral ativa na receita federal do Brasil. Desta forma, se faz necessário a verificação de regularidade em base de dados oficiais do MEC.

1.13.1 Vantagens do diploma digital

Segundo Grech e Camilleri (2017), os diplomas digitais possuem muitas vantagens sobre os diplomas em papel:

- A validação do diploma pode ser realizada de forma automática, sem intervenção humana.
- A segurança do diploma digital se baseia nos protocolos criptográficos, que asseguram que o certificado seja barato de produzir, mas extremamente caro para ser reproduzido por qualquer pessoa, exceto o emissor.
- Os diplomas digitais podem ser revogados pelo emissor.

- Certos tipos de fraude do emissor, como alterar, por exemplo, o número de registro, a data e hora, podem se tornar impossíveis dependendo do design do sistema.

1.13.2 Desvantagens do diploma digital

Os diplomas digitais também apresentam desvantagens significativas (Grech e Camilleri, 2017):

- Caso o registro falhe, os diplomas digitais se tornam inúteis, já que, diferentemente dos diplomas em papel, eles não têm valor intrínseco sem o registro.
- Sem o uso de assinaturas digitais, elas são extremamente fáceis de forjar.
- Quando são usadas assinaturas digitais, elas exigem o envolvimento de provedores de certificados de terceiros para garantir a integridade da transação, esses terceiros têm controle significativo sobre todos os aspectos do processo de certificação e verificação, que podem sofrer abusos.
- É mais fácil destruir registros eletrônicos - mantê-los em segurança requer sistemas de *backups* sofisticados e multicamadas que são propensos a falhas.
- Os registros de certificados digitais são propensos a vazamentos de dados em larga escala.

2 Desafios no serviço de emissão e validação de diplomas

2.1 Limitações do modelo atual proposto pelas portarias vigentes

Um dos principais objetivos da portaria N° 1.095/18 é tornar público a consulta e verificação das informações de diplomados de cursos superiores pela sociedade. Esse dispositivo se for cumprido pelas IES de forma permanente e contínua tem o potencial de resolver a fraude de diplomas fictícios. A tentativa de produzir uma imitação de um diploma verdadeiro, seria deflagrada por consulta pública. Desta forma, qualquer ação ilegal na fraude de um diploma sem a participação ou consentimento de uma IES poderia ser verificado e controlado pela sociedade.

Já os diplomas adulterados, seja na forma impressa ou digital, não serão necessariamente detectados por uma simples consulta no site da IES expedidora e/ou registradora, pois se for adulterada alguma informação no diploma que não seja um dado de consulta pública, como por exemplo, data de colação de grau, título e grau conferido, estas alterações não serão identificadas.

Se uma IES isolada, não registrar ou forjar o registro de um diploma expedido, ou até mesmo, após o registro de um diploma válido por uma IES registradora, manipular as informações do diploma, e mesmo assim publicar essas informações em seu site de consulta da IES expedidora, nestes casos, o dispositivo legal de consulta pública utilizando apenas o site da IES expedidora não seria eficiente para detectar uma fraude. No entanto, realizando a consulta pública na IES expedidora e na IES registradora e ainda solicitando um serviço de autenticidade na IES registradora para averiguar a assinatura eletrônica contida no diploma digital, desta forma, e desde que todos esses mecanismos sejam utilizados concomitantemente, assim, serviriam para verificação consistente (Tabela 7).

Tabela 7 – Tipos de fraudes resolvidas por dispositivos legais vigentes.

Tipo de fraude	Dispositivos legais vigentes	Nível de resolução
Diploma fictício	Consulta pública no site da IES	Resolve
Diploma adulterado	Consulta pública no site da IES e Diploma Digital	Resolve
Diploma ilegítimo	Consulta pública no site da IES expedidora e registradora e Diploma Digital	Resolve
Diploma extralegal	Consulta pública no site da IES expedidora e da IES registradora e Diploma Digital	Não resolve

Conforme apresentado na tabela acima a informação da IES registradora e sua assinatura digital contida obrigatoriamente no diploma poderão ser formas de validação e verificação quando confrontadas com as informações prestadas pela IES isolada seja em seu site ou por compartilhamento de seu signatário. A ampla publicidade e o site de validação de diploma poderão diminuir iniciativas criminosas de venda de diplomas sem a participação e consentimento das IES registradoras.

Embora o marco regulatório exposto acima, conceitualmente dispõe de mecanismos importantes de controle social, ele não resolve de forma definitiva e completa todos os tipos de fraudes discutidos e apresentados na tabela 4, como é o caso, do tipo de fraude extralegal, onde a fraude ocorre tanto na IES expedidora como na IES registradora.

2.2 Desafio no combate de fraude de diploma extralegal

As características da legislação brasileira, atribuem a IES registradora a responsabilidade de registro e de validação das informações contidas em um diploma, desta forma, estas IES podem, sejam por erros procedurais de validação da documentação enviada pela IES emissora ou equívocos cometidos por elas mesmas, ou ainda, por acordos ilegais, realizar o registro de diplomas de forma irregular. Ou seja, nestes casos, como as bases de dados dos registros de diplomas são propriedades da IES, a assinatura digital do diploma e a consulta pública nos sites da IES emissoras e registradoras são insuficientes para combater a fraude.

A gravidade e extensão desse problema podem ser comprovadas diante as portarias de medidas cautelares lançadas pelo MEC na abertura de processos administrativos contra IES registradoras, abaixo destacamos alguns casos.

Segundo a portaria N° 906/18:

> “Art. 4º A responsabilização da Fundação de Ensino Superior de Olinda (código e-MEC nº 281) pela guarda e gestão do acervo acadêmico da União de Escolas Superiores da FUNESO - UNESF (código e-MEC nº 1034), nos termos do art. 58 do Decreto nº 9.235, de 2017, respondendo o seu representante legal, nos termos da legislação civil e penal, inclusive nas hipóteses de negligência ou da utilização fraudulenta do acervo. ”
> “Art. 7 A identificação e o cancelamento imediato, pelo Instituto Superior de Educação de Pesqueira - ISEP (código e-MEC nº 2012), mantido pela Sociedade de Educação Cultura e Esportes de Pesqueira LTDA - ME (código e-MEC nº 1321), de eventuais diplomas expedidos de cuja análise fique evidenciada a sua irregularidade a partir da identificação de uma das seguintes situações, entre outras, que violem o marco regulatório educacional.”

Conforme a análise das portarias de medidas cautelares lançadas pelo MEC, a improbidade administrativa trata-se infelizmente de uma situação recorrente, demonstrando desta forma, a necessidade de combate a esse tipo de fraude em diplomas acadêmicos.

2.3 Desafio no uso do Diploma Digital

Um diploma digital só pode ser validado quando se verificam suas informações no livro de registro da IES registradora. Cada IES registradora regularmente ativa armazena seu livro de registro de forma proprietária e centralizada. Neste contexto, não há replicação e interoperabilidade da base de dados com outras IES. A disponibilidade dos dados ao público em geral para a finalidade de verificação dos diplomas depende do perfeito e contínuo funcionamento do banco de dados de cada IES. Neste caso, a tolerância a falhas é inversamente proporcional a quantidade de IES registradoras. Segundo informações do portal e-MEC há atualmente 497 IES

registradoras e, portanto, 497 pontos de falhas em potencial. Para as IES extintas a indisponibilidade de acesso ao seu banco de registro pode ocorrer no extravio dos dados no repasse das informações para o poder público ou no processo de salvaguarda destas informações.

2.4 Preservação digital

As IES devem manter os registros e documentos acadêmicos emitidos por elas de forma permanente, porém, pode ocorrer de uma determinada IES ser extinta e as informações do livro de registro dos diplomas serem extraviadas ou se tornarem de difícil acesso. Até o momento, segundo o e-MEC existem mais de 243 IES extintas.

De acordo com Miranda, Galindo e Vila Nova (2011) e Grácio (2012) constataram em suas pesquisas, poucas IES no Brasil possuem uma política de preservação digital, e que apenas algumas IES desenvolveram competência para assegurar o acesso a longo prazo aos seus acervos digitais, o que pode ser inferido pela falta de uma política institucional de preservação digital. Como as IES públicas e privadas não compartilham o mesmo fluxo e metodologia na emissão, registro e armazenamento de diplomas, segundo Silva e Mota (2012), a ausência de padrões, leis, modelos e normas aceleram a obsolescência tecnológica tanto dos objetos armazenados como dos seus próprios suportes.

3 Blockchain

O *blockchain* é uma base de dados distribuída, descentralizada, resistente a adulterações e na qual é possível apenas acrescentar dados. *Blockchain* não é uma nova tecnologia, mas um rearranjo de tecnologias existentes implementadas de uma nova maneira (Jirgensons e Kapenieks, 2018). Esta tecnologia surgiu com a criptomoeda Bitcoin para ser um *ledger*, armazenando todas as transações realizadas pelos usuários da criptomoeda, de forma a impedir o gasto duplo (uma quantia de dinheiro ser utilizada mais de uma vez).

Segundo Satoshi Nakamoto (2008), o *blockchain* em sua essência é uma autoridade de carimbo de tempo (TSA) distribuída que determina a ordem em que diversos eventos ocorrem e os armazena em uma rede ponto a ponto de nós não confiáveis, por meio de consenso distribuído em uma arquitetura de blocos encadeados.

Atualmente há diversos tipos de *blockchain*, conforme a tabela abaixo (Tabela 8).

Tabela 8 – Tipos de *blockchain* segmentados por modelo de permissão (Adaptado OECD, 2018).

		Ler	Escrever	Validar	Exemplo de utilização
Aberto	Público sem permissão	Aberto a qualquer um	Qualquer um	Qualquer um	Bitcoin Ethereum
	Público autorizado	Aberto a qualquer um	Participantes autorizados	Todos ou grupo de participantes autorizados	Sovrin
Fechado	Consórcio	Restrito a um grupo de participantes autorizados	Participantes autorizados	Todos ou conjunto de participantes autorizados	Vários bancos operando um livro razão compartilhado
	Privado autorizado ('enterprise')	Totalmente privado ou restrito a um grupo limitado de nós autorizados	Apenas o operador de rede	Apenas o operador de rede	Livro razão interno compartilhado entre controladora e subsidiárias

Segundo Lucena, Aurélio e Henriques (2017), uma das inovações do *blockchain* foi armazenar em um bloco o *hash* do bloco anterior e organizar as transações de um bloco em uma árvore Merkle. Assim, qualquer modificação em uma transação é percebida devido à mudança da raiz da árvore Merkle e qualquer

adulteração em um bloco é perceptível dado à discrepância que surge com o *hash* armazenado no cabeçalho do próximo bloco (Figura 1).

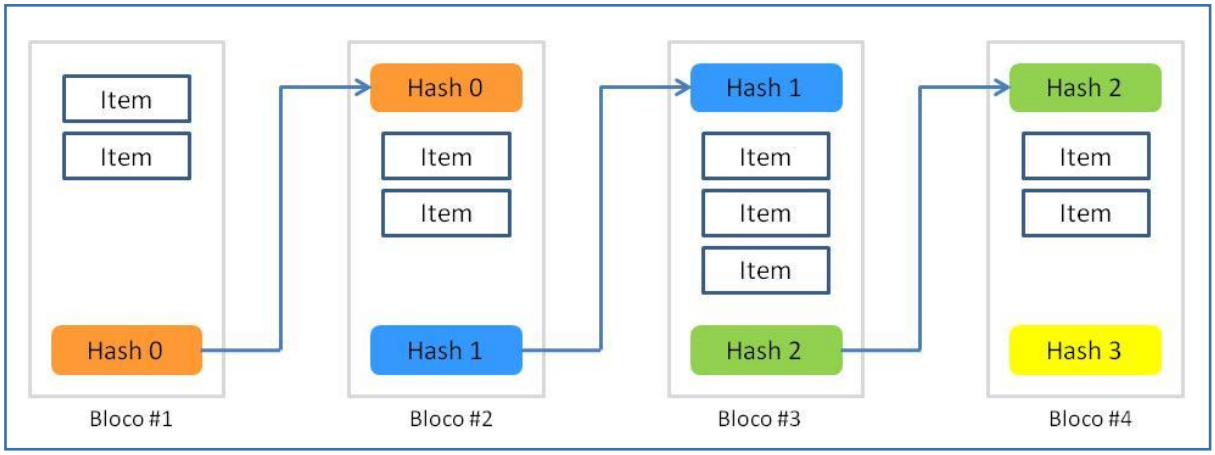


Figura 1 – Blocos encadeados no *blockchain* (Adaptado de Nakamoto, 2008).

3.1 Camadas do *blockchain*

Com base no estudo da literatura publicada por Couceiro, Gramoli e Romano (2017), podemos descrever a arquitetura da tecnologia *blockchain* em camadas. Apesar das camadas não serem totalmente independentes, podendo haver propriedades do *blockchain* comuns entre elas, as mesmas são distintas o suficiente para justificar uma abordagem por camadas, com o objetivo de obter uma melhor compreensão sobre o assunto (Figura 2).

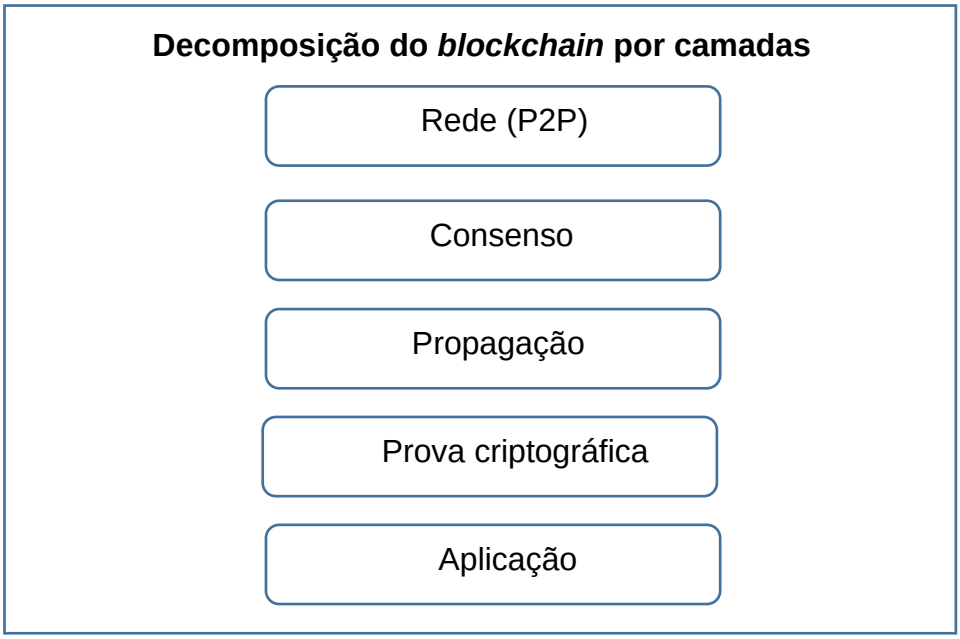


Figura 2 – Decomposição por camadas da tecnologia *blockchain*.

3.1.1 Rede P*eer-to-Peer* (P2P)

Esta camada consiste na infraestrutura fundamental do *blockchain*. A base é um protocolo de sistema distribuído que coordena o registro de dados e incentiva as partes a manter o consenso em uma base de dados compartilhada pelos nós de uma rede ponto a ponto decentralizada (Nakamoto, 2008). Nesta camada são definidas as regras de participação da rede e os níveis de acesso, leitura e escrita do banco de dados compartilhado (Tabela 8).

A descentralização da rede P2P se refere ao fato de não existir proprietário único da base de dados produzido pelos nós da rede, uma vez que todo nó da rede P2P é coproprietário, mantém a sua própria réplica do livro de registros e contribui para atualizar as outras réplicas (Braga, 2016).

Este sistema distribuído funciona sem necessariamente haver confiança nos participantes da rede. É possível atingir um consenso com incentivo de participação. O protocolo assegura que apenas cópias idênticas do *software* executados em cada nó participante possam interagir entre si.

3.1.2 Mecanismo de Consenso

De acordo com Aliaga *et. al* (2017), um mecanismo de consenso é um conjunto de passos que são dados por todos ou pela maioria dos nós para alcançarem um acordo sobre o estado do banco de dados distribuído num determinado momento de tempo. O mecanismo de consenso pode ser visto também como uma solução ao problema dos Generais Bizantinos (PGB).

Trata-se de um protocolo que descreve o formato da base de dados distribuída e como novos blocos de conteúdo são adicionados a esta base. Este protocolo descreve quais são as regras de incentivo dos nós participantes em atuarem como validadores e replicadores de novos registros de informação. A segurança da informação é alcançada na camada de consenso.

No *blockchain* todos os nós da rede P2P são envolvidos, de algum modo, na tomada de decisão de quais blocos de informação serão validados, registrados e replicados na rede. Trata-se, portanto, de um grupo (ou comunidade) decidindo em conjunto e de modo consensual.

A escolha do protocolo de consenso afeta a segurança e a escalabilidade do *blockchain*. Por essa razão, a arquitetura de um *blockchain* precisa ser modular para ser capaz de implementar diversos tipos de protocolos de consenso (Xu *et al.*, 2017).

Do ponto de vista de quem desenvolve aplicações sobre plataformas *blockchain* modernas, os métodos de consenso são uma funcionalidade, serviço ou configuração a ser habilitada e parametrizada (Braga, 2016). Os participantes das redes P2P obtêm consenso distribuído sobre a validade da transação e sobre o ordenamento delas.

3.1.3 Propagação na transação na rede distribuída

Esta camada tem como base um protocolo que determina como novos registros são transmitidos e propagados entre os nós da rede. Desta forma, permite que todos se comuniquem entre si em relação ao estado atual da rede. Os novos blocos de conteúdo válidos são produzidos através do mecanismo de consenso da rede.

3.1.4 Prova criptográfica

Trata-se de um protocolo que especifica como os novos blocos de conteúdo devem estar relacionados aos blocos anteriores. Esta camada define a estrutura de dados do bloco com o uso de uma variedade de técnicas criptográficas, incluindo funções *hash*, árvores Merkle e assinatura digital com base em infraestrutura de chave pública.

3.1.5 Aplicação

Esta camada consiste no código da aplicação que implementa as funcionalidades desejadas. As aplicações do *blockchain* possuem uma interface de usuário final, geralmente associado a aplicativos móveis e sistemas web. A camada de aplicação contém as regras de negócio e dados armazenados externamente ao *blockchain*, por meio de plataformas de s*oftwares* tradicionais e bases de dados comuns. Em geral, um sistema externo pode interagir com a base de dados distribuída ou com nós da rede através de *web services* para a integração entre a aplicação servidora (ou outros sistemas legados) e o *blockchain* (Braga, 2016).

3.2 Propriedades do *blockchain*

O *blockchain*, seja ele público ou privado, é tipicamente organizado em diferentes camadas. Ao nos referirmos a um tipo de *blockchain*, estamos discutindo a primeira camada (Rede P2P).

Ao segmentarmos o *blockchain* em várias camadas, podemos analisar melhor suas propriedades e avaliar onde elas precisam ser implementadas. De acordo com Bonneau *et al.*, (2015) estas propriedades são:

Segurança: Um nó da rede *blockchain* não pode arbitrariamente e de forma isolada adicionar informações no banco de dados compartilhado, sem a validação do mecanismo de consenso.

Disponibilidade: Os nós podem adicionar novos blocos ao livro com latência aceitável.

Estabilidade: Os nós da rede não devem alterar seu acordo prévio (consenso) de validação das informações sobre o registro dos dados.

Exatidão: Somente os blocos que representam transações válida podem ser adicionados ao banco de dados distribuído. Isto significa que todos os nós estão em conformidade com uma especificação de como os novos blocos podem se relacionar com os blocos anteriores.

3.3 Função *Hash*

Um *hash* ou função *hash* criptográfica é um algoritmo matemático que mapeia dados de tamanho variável para uma cadeia de *bits* de tamanho fixo (Schneier, 2004).

O *hash* é muito menor que o documento original e geralmente tem um tamanho fixo de dezenas (alguns têm centenas) de *bits*. A função *hash* é unidirecional, pois não é reversível, isto é, não é possível recuperar o documento original a partir da sequência binária do *hash* (Braga, 2016).

3.4 Estrutura de dados

Um bloco é uma estrutura de dados que reúne transações validadas por um protocolo de consenso para inclusão no *ledger*, o mesmo é composto por um cabeçalho, contendo metadados, seguido por uma longa lista de transações (Lin e

Liao, 2017). Um bloco pode ser identificado de duas maneiras, referenciando o *hash* do bloco ou referenciando a altura do bloco (Braga, 2016).

Cada bloco contém o *hash* de seu pai dentro de seu próprio cabeçalho. Há uma cadeia que vai todo o caminho de volta para o primeiro bloco criado, também conhecido como o bloco de gênese, ligado por uma sequência de *hashes*. O campo "*hash* do bloco anterior" está dentro do cabeçalho do bloco e, portanto, o *hash* do bloco atual é dependente do *hash* do bloco pai.

3.5 Árvore Merkle

Uma árvore Merkle é uma estrutura de dados usada para resumir e verificar eficientemente a integridade de grandes conjuntos de dados, estas estruturas são binárias e contêm *hashes* criptográficos (Rodrigues, 2017).

Uma árvore Merkle é construída por pares de nós de *hashes* recursivamente até que haja apenas um *hash*, chamado raiz, ou raiz Merkle. O algoritmo de *hash* criptográfico usado nas árvores Merkle simbólicas do Bitcoin, por exemplo, é SHA256 (Nakamoto, 2008).

Quando N elementos de dados são combinados e resumidos em uma árvore Merkle, é possível verificar se um determinado elemento está incluso na árvore com no máximo 2 * log2 (N) de cálculos, o que fornece uma maneira muito eficiente de verificar se a transação está de fato inclusa em um bloco (Lopez e Zhou, 2008).

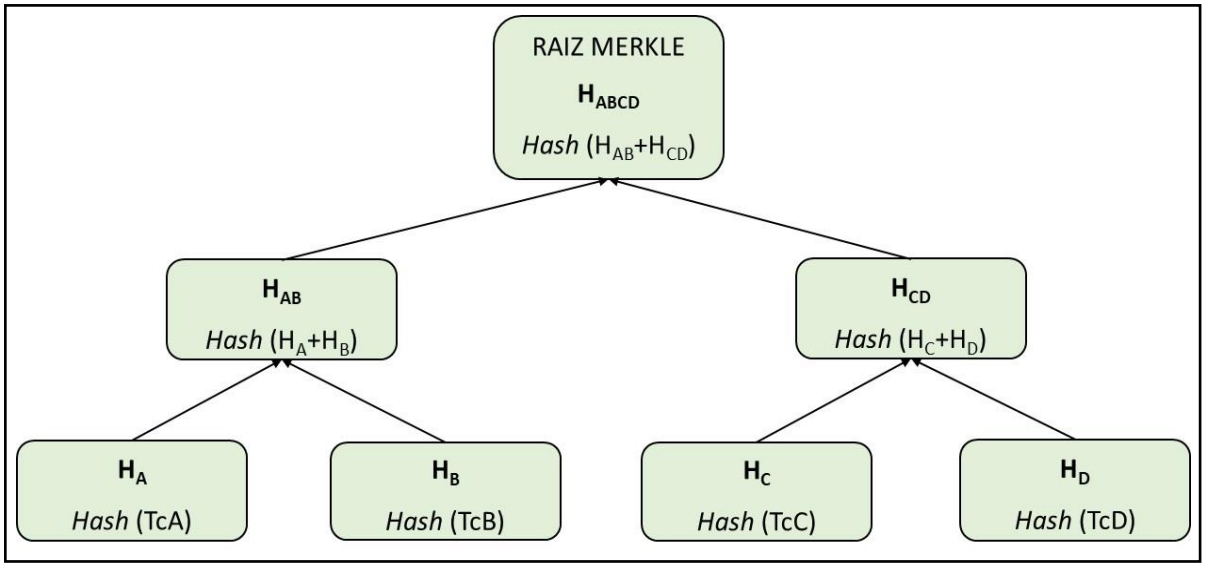


Figura 3 - Representação visual da árvore Merkle (Adaptado de Narayanan, 2016).

A árvore Merkle é construída de baixo para cima. Na Figura 3, começamos com quatro transações; chamadas de TcA, TcB, TcC, TcD. Essas transações não são armazenadas na árvore Merkle, e sim o *hash* resultante é armazenado em cada nó como H_A, H_B, H_C e H_D (Narayanan, 2016).

Pares consecutivos de nós são então mesclados em um nó pai, concatenando os dois *hashes* e combinando-os. O processo continua para cima até que haja apenas um nó no topo. Esse nó é conhecido como a raiz Merkle (H_{ABCD}).

3.6 Ledger

O *ledger* é um livro de registro físico ou digital utilizado por empresas e/ou instituições públicas para registrar a propriedade e/ou a transferência de ativos econômicos, contábeis e patrimoniais.

A transferência e registro de propriedade destes ativos registrados no livro razão são comumente denominadas transações. Segundo Grech e Camilleri (2017), um *ledger* são ferramentas pelas quais se pode determinar, em um dado momento, a propriedade de um ativo e de uma perspectiva técnica, é simplesmente uma lista de transações sequenciais, com registro de data e hora.

4 Estado da arte

Desde o advento do *blockchain* pelo Bitcoin e o surgimento de diversos tipos de mecanismos de consenso adequados a distintas aplicações, muitas empresas e governos estão explorando o uso de *blockchain* em áreas como: cadeia de suplementos, registros eletrônicos de saúde, votação, fornecimento de energia, gerenciamento de propriedade, gerenciamento de identidades entre outras (Lo *et al.*, 2018). Na área educacional, segundo Grech e Camilleri (2017), no que tange ao registro e emissão de diplomas acadêmicos, acredita-se que existe um grande potencial de uso do *blockchain*.

Uma prática comum para o gerenciamento de dados em sistemas baseados em *blockchain* é armazenar dados brutos fora do *blockchain*, enquanto metadados e *hashes* de dados primários podem ser armazenados dentro do próprio *blockchain*. Tal prática foi utilizada, em 2016 pelo MIT MEDIA LAB, pioneiramente desenvolvendo uma ferramenta (API), denominada Blockcert[1] de código aberto baseado na utilização do *blockchain* do Bitcoin para a emissão e registro de diplomas acadêmicos. A arquitetura da primeira versão desse trabalho era armazenar o *hash* de um diploma numa transação do Bitcoin e em sua segunda versão era possível emitir um certificado utilizando o *blockchain* público do Ethereum[2] (Nazaré, 2016).

Em 2017, a empresa SAP desenvolveu um sistema denominado de TrueRec, este sistema disponibiliza um aplicativo digital seguro e confiável para armazenar credenciais profissionais e diplomas acadêmicas baseadas no *blockchain* do Ethereum. O TrueRec foi disponibilizado inicialmente para as pessoas inscritas no curso *on-line Touch IoT* do SAP[3] (Klein, Prinz e Gräther, 2018).

No sistema federal de ensino Brasileiro foi apresentada um protótipo de uso de *blockchain* público na emissão de diplomas acadêmicos por Costa *et al*., (2018). Segundo este trabalho cada IES armazenaria seus diplomas de forma externa ao *blockchain*, usando *software* desenvolvido por fornecedor ou por elas mesmas.

1 https://www.blockcerts.org/
2 https://www.ethereum.org
3 https://www.sap.com/brazil/index.html

Essa abordagem, de acordo com Grech e Camilleri (2017), não garante um padrão de qualidade, segurança, preservação e interoperabilidade da base de dados. Desta forma, cada IES poderia criar ou utilizar diferentes *blockchains* para emitir e armazenar seus diplomas digitais, sem haver a interoperabilidade entre seus bancos de dados.

Em relação aos trabalhos citados acima uma questão importante para ser considerada na utilização do *blockchain* público na emissão e registros de diplomas acadêmicos, é que normalmente os *blockchains* públicos funcionam com o lastro de uma moeda virtual.

O custo de utilizar *blockchains* públicos, como por exemplo o *blockchain* do Bitcoin e do Ethereum para realizar o registro de diplomas está relacionado com o valor médio da taxa de transação paga pelos nós validadores da rede (mineradores). Na figura abaixo (Figura 4), podemos visualizar a grande variação da taxa de transação ao longo do período de um ano, por exemplo, a taxa do Bitcoin durante o período analisado, teve seu menor valor de USD 0.161 e sua maior valor foi de USD 6.557, isso representa uma variação de até 4070%. Já no *blockchain* do Ethereum observamos uma menor variação da taxa de transação, entretanto, a variação sofrida pode ser ainda de até, porém mesmo assim há variação é de até 2375%.

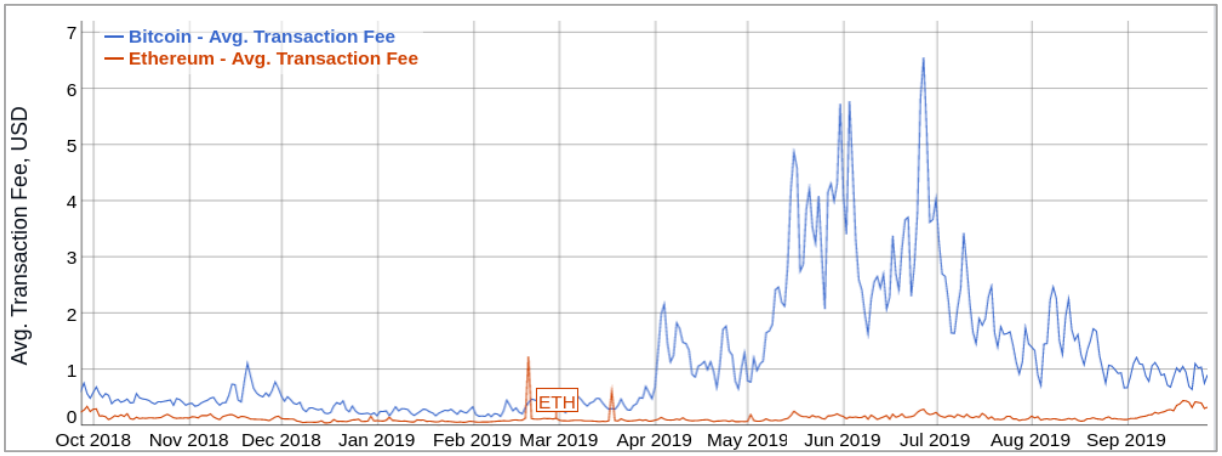


Figura 4 – Taxa média paga por transação no blockchain do Bitcoin e do Ethereum no período de um ano (Fonte: BitInfoCharts[1]).

1 /https://bitinfocharts.com/comparison/transactionfees-btc-eth.html#1y

Sendo assim, vale ressaltar, que como a variação do valor da taxa de transação está atrelada a compra e venda das criptomoedas, ou seja, trata-se de um fator totalmente externo ao mercado de expedição e registro de diplomas de curso superior no Sistema Federativo Brasileiro. Ou seja, todo incentivo de participação dos nós validadores, nestas redes tem como fundamento a recompensa nestes ativos virtuais. Logo, a preservação da base de dados depende do sucesso dessas moedas, o que pode trazer um risco extrínseco na preservação digital dos *hashes* dos diplomas digitais armazenados nestes *blockchains*.

Além disso, nem todos os tipos de *blockchains* têm a arquitetura adequada e recomendada para armazenamentos de informações que não sejam transações de suas moedas digitais. A cadeia de blocos do Bitcoin por exemplo, foi projetada exclusivamente como um meio para registrar pagamentos eletrônicos. A versão 0.9.0 do Bitcoin Core adicionou um novo tipo de transação padrão, concedendo acesso a uma função de *script* anteriormente não permitida *OP_RETURN.* Esta função aceita uma sequência definida pelo usuário de até 40 bytes. Uma sequência de 40 bytes é suficiente para codificar um identificador como um valor de *hash*. Esse valor pode representar exclusivamente qualquer documento digital, de uma imagem, um poema, ou qualquer outra estrutura abstrata de dados. (Apodaca, 2017). No entanto, o limite de 40 bytes no *OP_RETURN* restringe o uso da cadeia de blocos como um armazenamento de dados. Armazenar dados arbitrários no *blockchain* é dispendioso e é muito mais eficiente armazenar dados não monetários em outro local (Apodaca, 2017). No que diz respeito à eficiência de custos, desempenho e flexibilidade, as principais decisões de design ao usar um *blockchain* incluem a escolha de quais dados e cálculos devem ser colocados na cadeia de blocos e o que deve ser mantido fora do *blockchain* (Xu *et al.*, 2017).

5 A Pesquisa

Por força da lei, instituições de ensino superior isoladas podem escolher de forma livre e independente as IES universitárias para registrarem os diplomas de seus cursos superiores. Neste contexto, podem ocorrer acordos ilegais entre uma IES expedidoras e uma IES registradora e consequentemente, a fraude no registro de diplomas. Na forma como determina a lei, as IES registradoras, em parceria com as IES expedidoras, possuem o controle de todas as etapas de emissão, registro e armazenamento dos diplomas, desta forma, conforme relatado nos capítulos anteriores, podemos encontrar espaços para que ocorram abusos e desvios de função.

Com o objetivo de eliminar esse tipo de desvio de função, propomos organizar as IES (expedidoras e registradoras) numa rede P2P colaborativa de emissão e registro de diplomas. Nesta rede colaborativa, um mecanismo de consenso escolherá de forma transparente e imparcial a IES registradora que prestará o serviço de validação e registro dos diplomas a uma determinada IES expedidora.

Nossa proposta é apresentar o modelo conceitual de um mecanismo de consenso baseado em Prova de Reputação (PoR) para obtenção de um acordo no qual uma IES registradora conduzirá a validação do processo de registro de um lote de diplomas em uma determinada prestação de serviço.

O objetivo do mecanismo de consenso proposto consiste na descrição das regras codificadas e autorreguláveis que organizem a maneira na qual as IES do sistema federal de ensino possam colaborar entre si para validar e armazenar diplomas digitais de forma segura, transparente e com menor risco de fraudes.

O mecanismo de consenso poderá garantir que todas os diplomas armazenados sejam válidos e que cada registro seja adicionado e compartilhado por todas as IES do sistema federal de ensino participantes da rede. Atributos de eficiência, competividade e reputação permitem elevar o nível de segurança no processo de registro de diplomas. Sendo assim, as IES registradoras que por ventura, atuarem em algum processo de registro ilegal de diplomas, não estariam apenas sujeitas a sanções administrativas realizadas pelo MEC, mas também arriscando sua reputação e consequentemente os ganhos relativos ao serviço de registro de diplomas por ela realizado.

Desta forma, procuramos atribuir as características desejáveis de um novo mecanismo de consenso ao modelo proposto nesse trabalho. Segundo Aliaga *et. al* (2017), as características desejáveis de um novo mecanismo de consenso, são:

1) baixo consumo energético;
2) boa capacidade de armazenamento de dados;
3) escolha do grupo criador do bloco por sorteio (o grupo seria sorteado com maior chance para os usuários que estão há mais tempo em atividade na rede);
4) esquema de recompensa para os criadores de blocos;
5) esquema de punição para fraudadores;
6) ranqueamento dos usuários por reputação.

Em resumo, o mecanismo de consenso proposto neste trabalho consiste na escolha de uma IES registradora que conduzirá o processo de registro de um lote de diplomas expedido por uma IES isolada em uma determinada prestação de serviço, levando em consideração as características desejáveis de um novo mecanismo de consenso.

6 Modelo de mecanismo de consenso

6.1 Redes colaborativas

A colaboração entre organizações com o objetivo de obter soluções coletivas tem recebido crescente atenção desde o advento do *blockchain* do Bitcoin. As redes colaborativas têm sido estudadas a partir de diferentes abordagens teóricas (Grandori & Soda, 1995), entre elas, a teoria institucional estuda os fatores determinantes que fazem as organizações e instituições atuarem de forma cooperativa em uma rede de negócios. Esses estudos analisam os mecanismos institucionais pelos quais as relações inter-organizacionais são iniciadas, negociadas, coordenadas, monitoradas e concluídas.

Pela ótica da teoria institucional, se uma empresa ingressa em rede composta por empresas renomadas, poderá obter como resultado indireto o reconhecimento de ser uma instituição em conformidade com a legislação atual e operar com os padrões de qualidade dos demais parceiros. O tipo de necessidade que determina a formação de uma rede vai muito além de recursos materiais, sendo a dependência de legitimação fator preponderante, desta forma, as organizações buscam ganhar legitimidade no momento de participar de uma rede de cooperação (Balestrin, Verschoore e Reyes Junior, 2010).

As redes colaborativas apontam soluções organizacionais diversas das tradicionais, em que as conexões entre os agentes constituem relações estruturadas, socialmente e economicamente, no sentido de atender aos objetivos individuais e coletivos dos seus participantes (Olson, 1999). A articulação entre as diversas empresas da rede fortalece mutuamente os envolvidos, que passam a estar entrelaçados em relacionamentos com outras contrapartes identificáveis (Håkansson & Snehota, 1989).

Desta forma, as redes colaborativas podem ser definidas como o conjunto de transações repetidas e sustentadas por configurações relacionais e estruturais dotadas de fronteiras dinâmicas e elementos interconectados (Todeva, 2006), sendo assim, as redes colaborativas têm como pressuposto a interlocução de atores autônomos que, juntos, possam, a partir de uma relação cooperativa, unirem-se em prol dos interesses convergentes.

Portanto, o sistema federal de ensino pode ser representado por uma rede colaborativa no que tange ao registro e expedição de diplomas de cursos superiores. A ideia central do estabelecimento desta rede colaborativa é reunir fatores que permitam uma adequação a regulamentação vigente em uma única estrutura, sustentada por ações uniformizadas, porém descentralizadas, que viabilize ganhos competitivos pelas IES participantes e pela sociedade em geral.

6.2 Requisitos do mecanismo de consenso

Abaixo elencamos algumas premissas para que o mecanismo de consenso funcione adequadamente:

Infraestrutura básica

Um mecanismo de consenso é útil para obter um acordo sobre o estado de um banco de dados em um sistema distribuído. Desta forma, o mecanismo de consenso pode ser acoplado como um serviço de um *blockchain* privado ou de uma *Distribitued Ledger Technologies* (DLT), que conecta as IES registradoras e expedidoras em uma rede P2P. Esta infraestrutura básica pode ser criada e gerenciada através da contratação de redes de blockchain escaláveis utilizando a estruturas de código aberto, como por exemplo o Hyperledger Fabric e Ethereum.

Atualmente, existem diversas soluções disponíveis no mercado para a criação e gerenciamento de redes de *blockchain*, o que torna o cálculo da estimativa de custo de operação destas redes muito mais complexo, pois cada fornecedor define a estrutura de custos de forma diferente. Como por exemplo, a empresa Amazon (AWS) oferece um serviço denominado Amazon Managed Blockchain que por usa vez associa o valor deste serviço a diversos componentes da rede, sendo estes: associação à rede, instância de nós, armazenamento de nós e transferência de dados na rede.

Porém, para Brody *et al.* (2019), os custos totais inerentes de operação das redes de blockchain se apoiam em 4 variáveis: volume de transações, tamanho da transação, método de hospedagem e o protocolo de consenso. Considerando todos esses *inputs*, a média do custo de operação no *blockchain* privado é aproximadamente 5,6 vezes menor do que em um *blockchain* público. Ainda, de acordo com o estudo de Brody *et al.* (2019), o custo de uma transação em uma rede de *blockchain* privada é em torno de USD 0.858 enquanto o custo de transação de

uma rede de *blockchain* pública é em média de USD 5.061, ambos analisados no período de 5 anos com base no volume de 365.000 transações anuais sendo cada transação com o tamanho médio de 500 bytes. Vale ressaltar também, que o custo de operar uma rede de um *blockchain* privado é maior no primeiro ano, isso devido ao custo de implementação.

Rede P2P

Cada IES participante funciona como um nó da rede. O consenso distribuído será consistente quanto maior for o número de IES participantes. Atualmente há 201 IES universitárias que podem desempenhar o papel de validadoras. Logo, como a IES validadora neste protocolo de consenso é escolhido em cada rodada de validação a chance de se prever qual será a IES validadora de um lote de diplomas é 1/201.

Associação à rede

Nosso mecanismo de consenso requer uma camada de controle de acesso embutida nos nós da DLT (IES participantes). Os candidatos precisam passar por um processo de inscrição antes de ingressar na rede. Cada candidato tem um par de chaves criptográficas usado para autenticação e assinatura digital. A chave pública servirá como a identidade (ID) do participante.

6.3 Regras do mecanismo de consenso do livro de registro distribuído

Para ocorrer o registro de um diploma, a IES registradora realiza um processo de checagem das informações enviadas pelas IES isoladas e conferem se as exigências legais foram cumpridas. Uma vez que a transcrição de diplomas é autorizada e autenticada pela IES registradora, os dados do diploma são transcritos em seu livro de registro e propagados na rede para que as outras IES adicionem e atualizem seus respectivos livros de registros.

As IES da rede de cooperação proposta neste trabalho compartilham entre elas o livro de registros e há uma réplica do mesmo em cada unidade registradora e/ou emissora de todas IES participantes.

6.3.1 Definição de bloco e lote de diplomas

Uma IES expedidora por força da lei tem até 60 dias para emitir os diplomas dos alunos formados em seus cursos superiores a partir da data de colação de grau. As quantidades de diplomas expedidos variam de acordo com a quantidade de cursos e alunos formados em um determinado período acadêmico. Esta quantidade vamos designar como bloco de diplomas e dentro deste bloco os diplomas serão agrupados em lotes de tamanho limitado e variável.

O tamanho do lote é determinado a partir da disponibilidade da IES registradora no momento em que o consenso entra num acordo de qual será a IES registradora. Por exemplo uma IES registradora tem a disponibilidade no momento de registro de 500 diplomas, no entanto a IES isolada expediu um bloco com 1050 diplomas em um dado período acadêmico. Desta forma, o primeiro lote será formado de acordo com a disponibilidade da IES registradora escolhida como líder pelo mecanismo de consenso, logo, neste caso, o lote será de 500 diplomas. O tamanho do lote subsequente seguirá a mesma lógica e será determinado com base na disponibilidade da próxima IES registradora da fila. Se nesse caso a IES tiver disponibilidade de registro de 900 diplomas haverá mais um lote de 550 diplomas. Neste exemplo haverá um bloco de 1050 diplomas que contém dois lotes, um de 500 e outro de 550 diplomas respectivamente. Vale mencionar que o valor mínimo do lote pode ser de 1 diploma, não há restrição em relação a quantidade mínima, em determinadas situações por exemplo, a expedição de diplomas de mestrado ou doutorado, ou ainda apressamento de diploma, pode ser realizada em qualquer momento do período letivo, então a IES expedidora poderá demandar para registro apenas um diploma.

Logo, o lote é considerado limitado, pois seu tamanho dependerá da disponibilidade de registro da IES registradora e variável, pois se o registro for feito por mais de uma IES registradora, cada IES registradora pode possuir uma capacidade de registro diferente para o dado momento.

6.3.2 Estrutura de dados do lote de diplomas

O lote de diplomas será agrupado numa estrutura de dados que faz alusão aos blocos de dados do *blockchain* do Bitcoin. Ou seja, o *hash* de cada diploma digital

será agrupado numa estrutura de árvore Merkle, conforme descrito no item 3.5. Além disso, o lote terá um cabeçalho de metadados.

6.3.3 Descrição da fila de lotes de diplomas a serem registrados

As IES isoladas vão expedir os diplomas de seus concluintes conforme os calendários acadêmicos de seus respectivos cursos superiores. De forma que em um determinado momento haverá uma demanda variável de diplomas para serem registrados de diferentes IES isoladas.

O conjunto de diplomas expedidos e disponíveis para registro, de uma determinada IES isolada, entrarão em uma fila de lotes a serem registrados. As IES universitárias que são elegíveis a registrarem os lotes de diplomas são denominadas IES candidatas. A IES universitária escolhida pelo consenso da rede para conduzir a validação e registro dos diplomas, denominada IES líder, priorizará a ordem cronológica de envio do lote de diplomas na fila. As outras IES classificadas pelo mecanismo de consenso, porém não escolhidas pelo consenso para conduzir a validação e registros dos diplomas do lote, são chamadas de IES seguidoras (Figura 5)

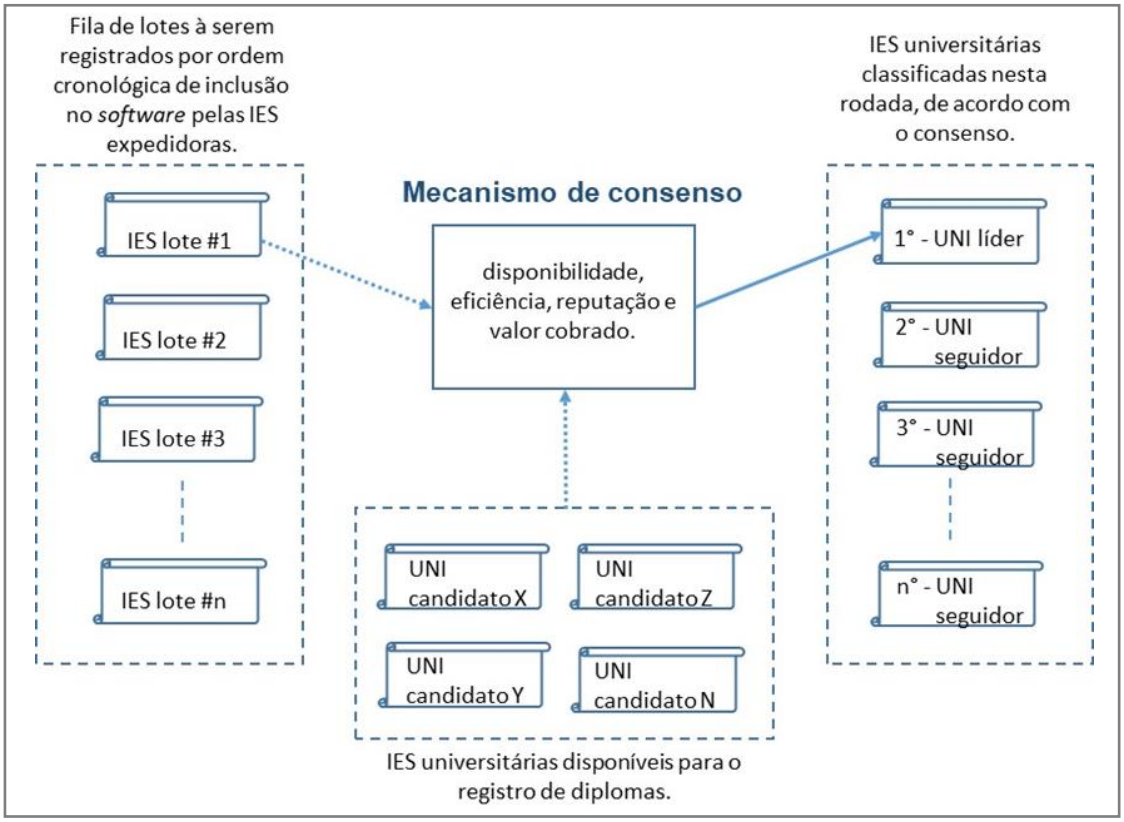


Figura 5 – Mecanismo de consenso para a escolha da IES registradora líder.

O processo de validação consiste em conferências de documentos, informações e verificações dos cumprimentos de exigências legais. Segundo Aparecida e Barbosa (2010), é comum nesse processo haver devoluções e solicitações de informações complementares para as IES isoladas. Nessas situações, os processos de registros dos diplomas do lote enviado para registro que tiverem alguma pendência serão cancelados e retornarão para a IES isolada revisá-los. Estes diplomas serão agrupados em um novo bloco e enviados novamente para a fila de registro. A cada novo pedido de registro é cobrado uma nova taxa de serviço quando ele for novamente inserido na fila de registros. Trata-se de uma situação praticada pelo mercado e isso deve ser considerado no mecanismo de consenso.

6.3.4 Critérios de seleção e classificação da IES líder

Durante o processo de escolha da IES líder, todos os nós (IES registradoras) assumem o papel de 'candidato'. Uma vez que o mecanismo de consenso escolhe uma IES registadora como líder, o nó vencedor da rodada assume o papel de 'líder' e esta tem o direito de validar e registrar os diplomas disponíveis na fila e todos os outros nós replicam em suas bases de dados os registros realizados pelo nó líder.

A qualquer momento, cada nó está em um dos três estados: líder, seguidor ou candidato. A validação de um lote de diplomas delimita uma etapa, denominado como rodada. Em cada etapa, o líder da rodada tem o direito de validar e registrar os diplomas de um lote de diplomas presentes na fila.

O processo de escolha da IES universitária líder da rodada será atribuída com base nos seguintes critérios de seleção e classificação:

- Disponibilidade;
- Eficiência da IES registradora;
- Reputação;
- Valor cobrado;
- IES registradoras não confiáveis.

Disponibilidade

Trata-se de uma métrica eliminatória. A IES registradora pode estar disponível para realizar o registro de diplomas desde que sua capacidade de registros não esteja

ao máximo sendo utilizada, ou ela pode ter atingido sua capacidade máxima de registro para o período e no momento estar indisponível para realizar novos registros. A IES registradora volta a ficar disponível assim que concluir o registro de um lote de diplomas anteriormente por ela captado.

Eficiência da IES registradora

Cada IES registradora tem uma capacidade singular de realizar a conferência da documentação exigida e de efetuar as transcrições das informações do diploma em seu livro de registro. Mesmo com um processo padronizado de checagem e verificação das informações, cada IES tem uma estrutura administrativa, como por exemplo, a quantidade de funcionários e recursos técnicos.

A capacidade de transcrição dos diplomas de uma IES registradora pode ser traduzida pela seguinte função:

Eficiência (q) = quantidade de diplomas registrados/45 dias

O denominador da função é o tempo máximo adequado que uma IES registradora teria para realizar a transcrição dos diplomas de uma IES isolada, considerando o prazo de mais 15 dias para realizar o pedido de uma eventual pendência de documentação ou algum outro problema que possa surgir no curso do processo.

Reputação

Reputação é uma opinião social acumulada durante um período de tempo sobre a imagem de uma determinada organização. A reputação, no caso, irá se basear na avaliação colaborativa sobre uma IES registradora em relação aos seus serviços prestados de registro de diplomas acadêmicos e o cumprimento das exigências legais que regulamentam este serviço.

A avaliação será medida através da coleta de opinião das IES expedidoras, ao fim de cada lote de diplomas registrados, tendo como objetivo atribuir uma nota ao serviço prestado pela IES registradora naquela interação. A nota do serviço será composta pelos seguintes parâmetros:

Tabela 9 – Parâmetros que compõe a nota do serviço prestado pela IES registradora a cada novo lote de diplomas.

Item	Parâmetros
1	Prazo de entrega do lote de diplomas registrados
2	Prazo para comunicar uma eventual pendência
3	Tempo para resolução de dúvidas e pendências
4	Histórico de checagem incorreta de documentos

Além disso, para compor a reputação, será conferido se a IES registradora em algum momento passou por algum processo administrativo instaurado pelo MEC envolvendo questões de ilegalidade no processo de registro de diplomas. De acordo com a Lei de Acesso à Informação (12.527/11), esses dados poderão ser coletados de maneira automatizada via *web service*.

Cada IES registradora possui um índice de reputação, que em conjunto com os critérios de seleção e classificação elencados acima, determinam sua elegibilidade e probabilidade de ser o nó validador e consequentemente registrador, em uma determinada iteração/rodada.

O índice de reputação (I(R)) será calculado com base na função abaixo:

I(R) = (3. média das notas obtidas pelos serviços prestados em cada interação) x (2. quantidade de processos administrativos acumulados desde a concepção da IES)

Valor cobrado

A cada novo bloco enviado para registro, a IES expedidora deverá fornecer o valor máximo que pretende pagar por registro de cada diploma. Desta forma, as IES registradoras candidatas serão apenas aquelas que atenderem esse pré-requisito. É importante salientarmos neste momento, que em hipótese alguma, a IES expedidora poderá escolher o valor exato de pagamento por registro de diploma. As IES registradoras que poderão “competir” por esse lote de diplomas a serem registrados, serão aquelas que oferecem o registro do diploma por valor menor ou igual ao solicitado. Desta forma, o mecanismo de consenso impede eventuais acordos feitos por fora da rede, e assim, evita que ocorra possíveis acordos ilegais.

IES registradoras não confiáveis

As IES registradoras, que por ventura se envolverão em fraudes de registro de diplomas e com processos administrativos em curso poderão ser automaticamente suspensas e ilegíveis no processo de escolha da IES líder pelo período determinado no processo administrativo instaurado pelo MEC. Entretanto, elas continuarão ativas na rede como nós seguidores, incorporando os blocos de diplomas validados pelas IES líderes em seu livro de registro.

6.3.5 Descrição da fila de IES registradoras

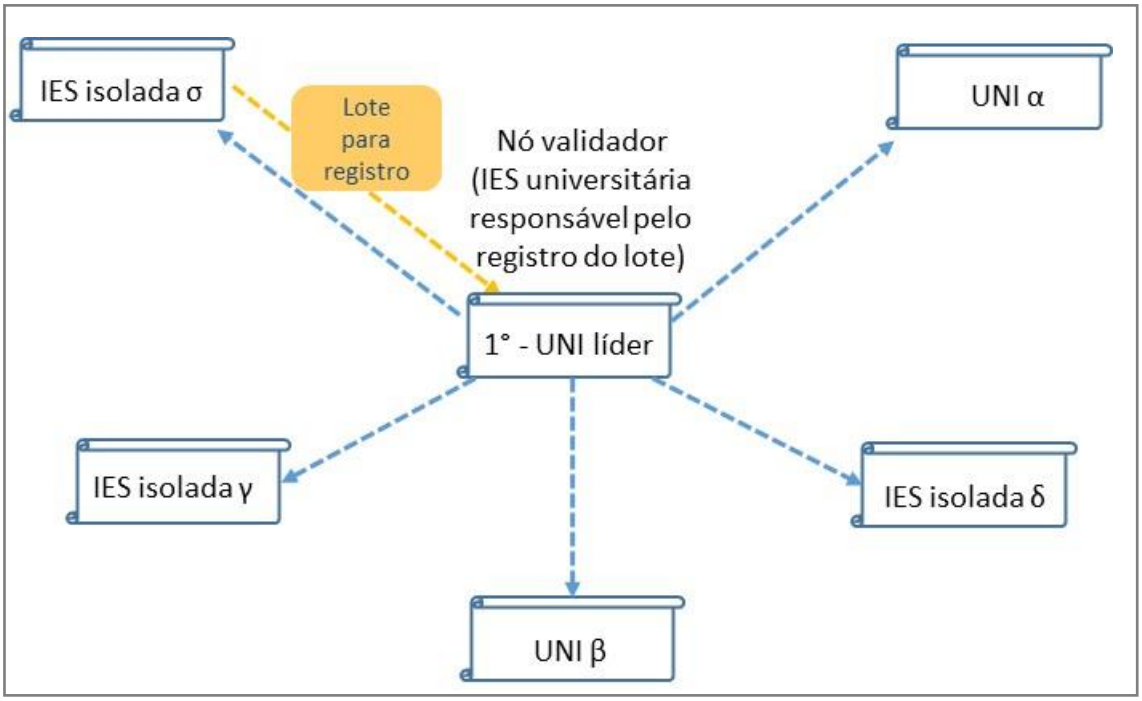
As IES universitárias são um subconjunto da rede e somente elas podem validar e registrar os diplomas expedidos pelas IES isoladas.

A IES líder da rodada, escolhida pelo mecanismo de consenso, valida e registra o lote de diplomas conforme sua disponibilidade e capacidade de registro. Como a demanda de diplomas expedidos é contínua durante o ano letivo e pode ser maior que a capacidade de atendimento da IES líder, o mecanismo de consenso executa um novo ciclo de classificação e escolha da próxima IES líder. Esse processo ocorre recursivamente e denominamos rodada de escolha da IES líder (Figura 5).

As IES expedidoras não sabem a princípio qual vai ser a IES validadora e registradora de seus diplomas. A condição da rede em não saber qual será o nó validador é uma característica de protocolos de *blockchain*. De acordo com Qin e Gervais (2018), uma das diferenças fundamentais entre banco de dados centralizados e um *blockchain* é que o nó validador do bloco da rodada é selecionado de acordo com o mecanismo de consenso dentre todos os nós candidatos descentralizados.

O processo de registro se inicia com a validação do lote de diplomas pela IES líder registradora, em seguida, as informações são transcritas para o livro de registro da IES registradora validadora da rodada e, então, a mesma realiza um *broadcast* na rede para transmitir os novos registros para todos os nós participantes da rede. Após o recebimento dos novos registros, todas as IES da rede atualizam automaticamente o seu livro de registro, de modo que os novos registros passam a fazer parte do livro de registro de cada IES (Figura 6)

Figura 6 – Processo de replicação dos novos registros de diplomas entre as IES participantes.



Diferentemente do sistema atual de registro de diplomas, onde, o número de registro do diploma é sequencial para cada livro de registro e consequentemente para cada IES, no modelo proposto, o número de registro do diploma passará a ser sequencial considerando todos os livros de registros de todas as IES, ou seja, passará a existir uma sequência única de registro de diplomas do sistema federal de ensino.

6.3.6 Incentivos do mecanismo de consenso

Conforme apresentado nos capítulos anteriores, atualmente as IES registradoras já cobram e recebem um valor para a execução do serviço de registro de diplomas. O mecanismo de consenso poderá aumentar o ganho das IES registradoras que tiverem um melhor desempenho e qualidade na execução desse serviço.

Para as IES isoladas o mecanismo de consenso escolherá com base no menor preço do serviço cobrado pelas IES registradoras. Isso apresenta-se como uma vantagem significativa para as IES isoladas, pois podem desembolsar menos pelo serviço de registro.

6.4 Benefícios para a sociedade e o sistema de ensino

A solução proposta ajuda a superar as limitações do sistema atual, permitindo que as instituições acadêmicas armazenem diplomas e históricos escolares de forma permanente e segura em um livro de registro distribuído e compartilhado, em vez de bancos de dados centralizados.

A solução oferece segurança e transparência na emissão e registro de diplomas realizadas no ambiente digital. AS IES participantes atuam como autoridades verificadoras, garantindo que cada diploma expedido seja emitido, registrado e validado de forma confiável e imutável.

O diploma ainda pode ser consultado mesmo que a instituição que o emitiu não exista mais ou não tenha mais acesso ao diploma emitido. O registro dos diplomas emitidos utilizando a infraestrutura do *blockchain* só podem ser destruídos se todas as cópias em todos os computadores das IES participantes que hospedam o *software* forem destruídas.

Neste cenário o mecanismo de consenso pode ser entendido como um conector sofisticado de livros de registros das IES públicas e privadas. Ele transfere o risco e a responsabilidade da execução de código e armazenamento de dados centralizados das IES para redes descentralizadas e confiáveis.

Além disso, o livro de registro de diplomas será compartilhado entre todas as IES participantes da rede, logo haverá um número de registro único, o que futuramente poderá prover a consulta pública de diplomas em um único sítio eletrônico.

7 Discussão

Este trabalho teve como tema compreender os desafios e limitações do sistema federal de ensino na prestação dos serviços de validação e registro de diplomas acadêmicos pelas IES. Para isso, delimitamos a extensão desse estudo, propondo uma taxonomia que classifica diferentes tipos de fraudes de diplomas. Com base na taxonomia elaborada foi feita uma análise e contextualização dos principais pontos de fragilidade do sistema atual frente aos anseios sociais e regulatórios e das novas demandas de proteção e preservação das informações e dados pessoais, de acordo com a LGPD.

No decorrer do trabalho foi observado que as portarias N° 315/18, N° 1095/18 e Nº 554/19 indicam a necessidade da transformação digital das IES, entretanto, a simples adoção de tecnologias como, digitalização da documentação acadêmica, assinatura digital e portais acadêmicos para a publicidade de informações de diplomados de cursos superiores, que são os meios existentes atualmente são insuficientes no combate a fraudes de diplomas. Embora a assinatura eletrônica possa garantir a autenticidade e integridade do diploma digital expedidos pelas IES, ela não garante a transparência e veracidade no processo.

Neste contexto, é fundamental que haja uma reorganização e padronização do processo de emissão, validação e registro de diplomas, em específico no modo de como é feito a prestação de serviço entre as IES registradoras e expedidoras. Diante desse cenário, a tecnologia de *blockchain* tem o potencial de colaborar para a padronização e transparência do processo. Entretanto, notamos que o custo inerente do processo de validação de *blockchains* públicos com lastro em criptomoedas sofre muita variação, tornando um fator imprevisível e consequentemente dificultando a utilização dos mesmos para emissão e registro de diplomas. Além disso, para criar uma rede colaborativa com vantagens significativas de participação das IES do sistema federativo, respeitando-se a legislação vigente faz-se necessário um mecanismo de consenso específico para a funcionalidade de emissão, validação e registro de diplomas acadêmicos

Desta forma, esse trabalhou contribuiu na análise de como o sistema federal de ensino (IES expedidoras e registradoras), pode se organizar, respeitando a legislação vigente, numa rede ponto a ponto colaborativa de emissão e registro de diplomas.

Na rede colaborativa proposta, o mecanismo de consenso escolhe de forma transparente e imparcial a IES registradora que prestaria o serviço de validação e registro dos diplomas a uma determinada IES isolada. A principal contribuição deste trabalho é o modelo conceitual de um mecanismo de consenso baseado em Prova de Reputação (PoR) para obtenção de um acordo no qual uma IES registradora conduzirá a validação do processo de registro de um lote de diplomas em uma determinada prestação de serviço. O objetivo do mecanismo de consenso proposto consiste na descrição das regras codificadas e autorreguláveis que organizem a maneira na qual as IES do sistema federal de ensino possam colaborar entre si para validar e armazenar diplomas digitais de forma segura, transparente e com menor risco de fraudes.

O diploma validado pelo mecanismo de consenso proposto terá a característica de ser uma representação fiel ao diploma registrado e este será imutável e resistente ao tempo, além de ser compartilhado para toda a rede colaborativa, tornando as informações dos diplomas, mesmo das IES inativas facilmente consultáveis. Entretanto, caso ocorra desvio de função ao emitir o diploma pela IES expedidora e não seja detectado pela IES registradora, como por exemplo, em caso de diploma registrado de algum aluno sem lastro acadêmico confiável, infelizmente o mecanismo de consenso não detectará.

Essa questão, nos mostra que se faz necessário, agregar no futuro a este modelo de mecanismo de consenso a utilização de *smart contracts,* que são contratos regidos apenas por código, em plataformas de *blockchain* que são executados automaticamente assim que as condições contratuais acordadas pelas partes envolvidas sejam cumpridas.

Neste contexto tecnológico muitas etapas do ensino-aprendizagem, como por exemplo, avaliações, frequência do aluno, participação de atividades curriculares, entrega de trabalhos acadêmicos, poderiam ser registradas automaticamente e estas informações auditáveis fariam parte da trajetória acadêmica e consequentemente, uma vez que essas etapas estejam validadas, fundamentariam de forma mais confiável o diploma acadêmico.

Desta forma, a evolução do modelo de mecanismo de consenso proposto poderia se apoiar na possibilidade de registrar e validar não somente o documento final, mas todas as etapas do processo. Dessa maneira, a *Blockchain* permite a interação autônoma entre as partes, a IES e o aluno, sem a necessidade de terceiros,

como por exemplo, cópias autenticadas em cartório, que são documentos não necessariamente verdadeiros, pois em uma cópia autenticada, apenas é confrontado a cópia com o documento apresentado, garantindo desta forma, a autenticidade da cópia. Porém, não há garantia que o documento apresentado seja verdadeiro.

O mecanismo de consenso proposto nesse trabalho permite que as IES do sistema federal de ensino possam trabalhar em conjunto a partir da infraestrutura de uma rede descentraliza como um *blockchain*. Todo o gerenciamento de identidade e dados sensíveis privados dos alunos e ex-alunos dos seus cursos superiores poderiam ser realizados com base na permissão concedia do aluno as referidas informações a partir do *blockchain*. Em vez de compartilhar explicitamente seus dados com a própria IES, terceiros ou empresas eles forneceriam sua chave pública para acesso a suas informações armazenadas no *blockchain*. Esta chave poderia ser revogada a qualquer momento, conforme a decisão do titular dos dados.

Além da possibilidade de revogação da chave pública que impossibilita o acesso aos dados particulares armazenados no *blockchain*, uma outra característica técnica interessante seria o compartilhamento de visualizações dos dados em vez de propriamente os dados originários ou primários. Por exemplo, um ex-aluno poderia em tese, escolher as informações acadêmicas que deseja compartilhar, com uma empresa na qual esteja participando de um processo seletivo.

A princípio, o funcionamento do compartilhamento de visualizações dos dados seria também com base no compartilhamento da chave-pública do titular dos dados, cada visualização feita pelo titular teria respectivamente uma chave de acesso atrelada. A partir da Lei 13.853, (Lei Geral de proteção de dados, LGPD) cada vez mais organizações públicas e privadas irão viabilizar meios digitais para que o titular dos dados tenha acesso aos seus dados pessoais que estão sendo coletados e tratados por elas.

As IES, por outro lado, não armazenariam nenhuma informação em um banco de dados central corporativo e, portanto, a expedição e registro de diplomas acadêmicos proposto nesse trabalho poderiam trazer benefícios as IES na mitigação de riscos relacionados com as prerrogativas da LGPD, no tocante a privacidade e as atividades relacionadas no tratamento de dados de alunos e ex-alunos de seus cursos superiores.

7.1 Limitações

Garantir a validade de um diploma acadêmico não é apenas assegurar a sua autenticidade e integridade. Pois como vimos anteriormente, o diploma representa uma trajetória acadêmica onde todas as etapas acadêmicas foram realizadas e cumpridas num determinado contexto curricular. Entretanto, com o mecanismo proposta atualmente, não há maneiras de validar que o diploma emitido decorre de uma trajetória acadêmica confiável.

Porém, esta realidade tecnológica não está obstante, e reside na utilização de plataformas de *smart contracts*. Desta forma, conforme haja um amadurecimento tecnológico destas plataformas de *smart contracts* será possível refinar e complementar o mecanismo de consenso proposto neste trabalho para abranger o registro e validação de toda as etapas de uma trajetória acadêmica e não somente o documento final, o diploma.

O mecanismo de consenso proposto abrange a prestação de serviço de registro de diplomas entre IES universitárias e IES isoladas, no entanto o modelo apresentado não incluí a validação e registro das IES do tipo 2 (Centro universitários) na rede ponto a ponto apresentada neste trabalho. Além disso, também não estão incluídos a validação e registro dos diplomas das próprias IES universitárias.

7.2 Trabalhos Futuros

A partir das discussões realizadas nesse trabalho, contribuímos com a estruturação de uma temática de estudo que pode ser ramificar nos seguintes pesquisas e trabalhos futuros:

1. Avaliar o mecanismo de consenso proposto com base em simulação computacional.
2. Refinar e abranger o mecanismo de consenso para a validação e registro dos diplomas das IES do tipo 1 (universidades) e do tipo 2 (Centros universitários).
3. Implementação de prova de conceitos do modelo proposto e elaboração de estudos de casos.
4. Investigar de forma específica a utilização de *smart contract* no registro e validação de toda a documentação pertencente a trajetória acadêmica do aluno.

7.3 Conclusão

Conforme analisado no decorrer do estudo, fraudes de diplomas acadêmicos é um problema interdisciplinar e complexo que envolve a articulação de tecnologias da informação, inovação da gestão das IES públicas e privadas e o monitoramento constante dos órgãos fiscalizadores e da sociedade em geral, mas sobretudo para se criar esse contexto é necessário primeiramente surgir pesquisas científicas direcionadas que combinem diferentes abordagens e áreas de estudos.

Portanto, este trabalho contribuiu no avanço da compreensão de como as fraudes de diplomas acadêmicos ocorrem e no legado de uma taxonomia que pode servir de base para se criar um vocabulário específico neste campo de estudo. Além do vocabulário e análise das fraudes de diplomas este trabalho avançou sobretudo na proposta de um modelo conceitual de mecanismo de consenso que descreve como as IES do sistema federal de ensino podem compartilhar, emitir e registrarem diplomas acadêmicos de forma segura e resistente a fraudes.

O uso de tecnologias como o *blockchain*, para a emissão, validação e registro de diplomas ainda está em estágio embrionário de aplicação, sendo assim, nosso trabalho é uma referência importante do primeiro mecanismo de consenso formulado especificamente para a realidade do nosso sistema federal de ensino.

Enfim, a contribuição deste trabalho além de criar as bases para futuras pesquisas que possam se aprofundarem nesta temática, propõe uma solução que pode ser o referencial inicial da aplicação do *blockchain* na validação e registro de diplomas nas IES do Brasil, padronizando este processo e inviabilizando fraudes em certificações acadêmicas.

8 Referências

APARECIDA, R.; BARBOSA, F. Universidade Federal de São Carlos. 2010.

APODACA, R. **OP_RETURN and the Future of Bitcoin**. Disponível em: <https://bitzuma.com/posts/op-return-and-the-future-of-bitcoin/>. Acesso em: 5 mar. 2019.

BALESTRIN, A.; VERSCHOORE, J. R.; REYES JUNIOR, E. O campo de estudo sobre redes de cooperação interorganizacional no Brasil. **Revista de Administração Contemporânea**, v. 14, n. 3, p. 458–477, 2010.

BONNEAU, J. *et al.* SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. **Proceedings - IEEE Symposium on Security and Privacy**, v. 2015- July, p. 104–121, 2015.

BRAGA, A. M. Segurança e Desenvolvimento de Software . Introdução. **Cpqd**, p. 34, 2016.

BRODY, P. *et al.* **Total cost of ownership for blockchain solutions**. [s.l: s.n.]. Disponível em: <https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf>.

EDUARDO, Y.; ALIAGA, M.; LEAL, V. C. Avaliac ¸ a busca de nova estrat ´ egia mais eficiente e segura. 2017.

GRECH, A.; CAMILLERI, A. F. A. **Blockchain in Education**. [s.l: s.n.].

GROLLEAU, G.; LAKHAL, T.; MZOUGHI, N. An Introduction to the Economics of Fake Degrees. **Journal of Economic Issues**, v. 42, n. 3, p. 673–693, 2016.

JIRGENSONS, M.; KAPENIEKS, J. Blockchain and the Future of Digital Learning Credential Assessment and Management. **Journal of Teacher Education for Sustainability**, v. 20, n. 1, p. 145–156, 2018.

KLEIN, S.; PRINZ, W.; GRÄTHER, W. A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities.

Proceedings of the ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies, n. 10, p. 1–8, 2018.

LIN, I. C.; LIAO, T. C. A survey of blockchain security issues and challenges. **International Journal of Network Security**, v. 19, n. 5, p. 653–659, 2017.

LO, S. K. *et al.* Evaluating Suitability of Applying Blockchain. **Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS**, v. 2017-Novem, n. November, p. 158–161, 2018.

MALAMUD, C. **Open Government Working Group**. Disponível em: <https://public.resource.org/8_principles.html>.

NAZARÉ, J. **What we learned from designing an academic certificates system on the blockchain**. Disponível em: <https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196#.p7gda76v4>. Acesso em: 11 jul. 2019.

OECD. OECD Blockchain Primer. 2018.

QIN, K.; GERVAIS, A. An overview of blockchain scalability , interoperability and sustainability. [s.d.].

QUEIROZ, A. L. **Uma Solução de Software de Assinatura Digital de Documentos para Instituição de Ensino Brasileira**. [s.l: s.n.].

SILVA JUNIOR, LAERTE PEREIRA DA; MOTA, V. G. DA. Políticas de preservação digital no Brasil : características e implementações. **Ciência da Informação**, v. 41, n. 1, p. 51–64, 2012.

XU, X. *et al.* A Taxonomy of Blockchain-Based Systems for Architecture Design. **Proceedings - 2017 IEEE International Conference on Software Architecture, ICSA 2017**, n. April, p. 243–252, 2017.