UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
UNIDADE ACADÊMICA DE GARANHUNS

ANDERSON MELO DE MORAIS

CONTROLE DE EMISSÃO E VALIDAÇÃO DE DIPLOMAS DIGITAIS UTILIZANDO BLOCKCHAIN

Garanhuns
2019

ANDERSON MELO DE MORAIS

CONTROLE DE EMISSÃO E VALIDAÇÃO DE DIPLOMAS DIGITAIS UTILIZANDO BLOCKCHAIN

Trabalho de Conclusão de Curso submetido à Universidade Federal Rural de Pernambuco - Unidade Acadêmica de Garanhuns, como requisito necessário para obtenção do grau de Bacharel em Ciência de Computação, sob a orientação do prof. Ms. Sérgio Francisco Tavares de Oliveira Mendonça.

Garanhuns
2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Ariano Suassuna, Garanhuns-PE, Brasil

M827c Morais, Anderson Melo de
Controle de Emissão e Validação de Diplomas Digitais Utilizando Blockchain / Anderson Melo de Morais. - 2019.
66 f. ; il.

Orientador: Sérgio Francisco Tavares de Oliveira Mendonça.
Trabalho de Conclusão de Curso (Graduação em Ciência da Computação)-Universidade Federal Rural de Pernambuco, Departamento de Ciência da Computação, Garanhuns, BR-PE, 2019.
Inclui referências e anexo(s)

1. Computação 2. Computadores – medidas de segurança 3. Blockchains (Base de dados) I. Mendonça, Sérgio Francisco Tavares de Oliveira , orient. II. Título

CDD 004

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

ANDERSON MELO DE MORAIS

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Ciência da Computação, sendo aprovado em sua forma final pela banca examinadora:

Orientador: Prof. Sérgio Francisco Tavares de Oliveira Mendonça
Universidade Federal Rural de Pernambuco - UFRPE

Prof. Fabiano Barbosa Mendes da Silva
Universidade Federal Rural de Pernambuco - UFRPE

Prof. Diogo de Lima Lages
Universidade Federal Rural de Pernambuco - UFRPE

Garanhuns, 25 de janeiro de 2019

Este trabalho é dedicado a Virgem Maria Mãe de Deus,
que tudo o que eu tenho Vos pertença para a maior glória do Senhor Jesus.

Agradecimentos

Sou grato a Deus, que me permitiu concluir este trabalho e por sua graça me fazer chegar ao fim desta graduação.

A minha mãe, que sempre deu a vida por mim, acreditou em meu potencial e me incentivou a ir sempre mais longe.

Ao meu orientador o prof. Sérgio Mendonça, que se propôs a construir este trabalho comigo, sou muito grato por sua disponibilidade, incentivo e pelas valiosas lições que aprendi ao longo desses meses, as levarei sempre comigo.

Ao prof. Robson Santos, que contribuiu muito para a minha formação acadêmica.

A Maria Simone, que esteve ao meu lado durante toda a graduação, comemorando comigo as realizações e me motivando nos momentos difíceis.

A minha amiga Viviane Cristina, que sempre esteve ao meu lado desde o inicio do curso.

Por fim, a todos os que, direta ou indiretamente, contribuíram para a conclusão dessa etapa.

Resumo

Com o desenvolvimento de novas tecnologias surgem também novos desafios em relação a segurança das inúmeras informações que são geradas constantemente. Este trabalho tem como objetivo principal avaliar a viabilidade do uso de Blockchain para garantir segurança na emissão de diplomas digitais por Instituições de Ensino Superior e desenvolver uma aplicação para exemplificar o processo de emissão e validação de um documento digital. Para isso, realizou-se uma pesquisa bibliográfica para entender o funcionamento de uma rede Blockchain e qual o nível de segurança apresentado por ela, também buscou-se compreender como se dá o processo de emissão de um diploma e quais os mecanismos de segurança tradicionalmente utilizados para a proteção de dados. Em seguida foi realizada a implementação de um sistema web, utilizando ferramentas modernas de desenvolvimento, com o intuito de demonstrar a emissão de um diploma digital e a utilização de uma rede Blockchain local para o registro deste documento. A aplicação permite ainda, a validação de documentos emitidos, utilizando-se de um sistema de consulta em múltiplos níveis, que verifica se o documento se encontra registrado na base de dados da aplicação e na Blockchain local, para só então confirmar a sua autenticidade.

Palavras-chave: Blockchain. Segurança da informação. Diplomas digitais.

Abstract

With the development of new technologies, new challenges also arise regarding the security of the many information that is constantly generated. This paper aims to evaluate the feasibility of using Blockchain to guarantee security in the issuance of digital diplomas by Higher Education Institutions and to develop an application to exemplify the process of issuing and validating a digital document. For this, a bibliographical research was carried out to understand the operation of a Blockchain network and the level of security presented by it, also sought to understand how the process of issuing a diploma is given and what security mechanisms traditionally used for data protection. Next, a web system was implemented, using modern development tools, in order to demonstrate the issuance of a digital diploma and the use of a local Blockchain network to register this document. The application also allows the validation of documents issued using a multi-level query system, which verifies that the document is registered in the application database and the local Blockchain, only to confirm its authenticity.

Keywords: Blockchain. Information security. Digital Diplomas.

Lista de ilustrações

Lista de tabelas

Lista de códigos

Lista de abreviaturas e siglas

IoT	Internet of things
IDS	Intrusion detection System
IPS	Intrusion prevention system
ICP	Infraestrutura de Chaves Públicas
ITI	Instituto Nacional de Tecnologia da Informação
TCLE	Termo de Consentimento Livre e Esclarecido

Sumário

1 Introdução

Nos dias de hoje, torna-se cada vez mais comum a utilização de sistemas distribuídos para atender as mais diversas demandas que surgem na vida das pessoas. Segundo Tanenbaum (2007), "um sistema distribuído é um conjunto de computadores independentes, que se apresentam aos seus usuários como um sistema único e coerente", e são amplamente utilizados em sistemas de pesquisas (motores de busca), sistemas financeiros, jogos online, redes sociais, entre muitas outras coisas.

Em uma sociedade casa vez mais informatizada e dependente da tecnologia, uma preocupação crescente se dá em relação a segurança dos dados e a integridade das informações que são transacionados a todo momento. Para que um sistema computacional seja seguro ele precisa, dentre outras coisas, ser confiável, ou seja, deve atender, de forma fidedigna, as expectativas que temos em relação aos seus serviços (TANENBAUM, 2007).

Uma estratégia que pode ser utilizada para garantir a segurança e a confiabilidade dos dados se dá através da utilização de redes Blockchain (NAKAMOTO, 2008), que funcionam como um tipo de base de dados distribuída que guarda registros de transações em uma estrutura de blocos encadeados e criptografados, onde cada novo bloco gerado guarda uma referência para o seu anterior. Assim, para que as informações armazenadas em um bloco fossem alteradas seria necessário gerar novamente todos os blocos posteriores a ele, o que em uma rede de grandes proporções se tornaria inviável do ponto de vista computacional.

1.1 Motivação

No Brasil, ao concluir um curso, seja ele de grau técnico, superior ou de pós-graduação, o aluno tem o direito de receber um diploma que lhe servirá como prova da formação recebida e, tendo validade nacional, lhe permitirá exercer sua profissão.

Segundo afirma o Artigo 48 da Lei 9394/96 - Lei de Diretrizes e Bases da Educação Nacional (BRASIL, 1996) "Os diplomas de cursos superiores reconhecidos, quando registrados, terão validade nacional como prova da formação recebida por seu titular"(BRASIL, 1996). Afirma também no § 1º que "Os diplomas expedidos pelas universidades serão por elas próprias registrados, e aqueles conferidos por instituições não-universitárias serão registrados em universidades indicadas pelo Conselho Nacional de Educação"(BRASIL, 1996). No entanto esse registro dos diplomas e certificados expedidos por cada universidade se dá apenas de maneira manual, fazendo uso de livros de registros, o que pode acarretar em alterações, inclusões indevidas nos livros, entre outras coisas. Além disso há a dificuldade

de verificar a autenticidade de um documento já emitido, o que dá possibilidade a pessoas mal intencionadas de falsificarem diplomas e os comercializarem.

O Código Penal brasileiro classifica como criminoso o ato de "Art. 297 – Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro"(BRASIL, 1940), e determina uma pena de reclusão, de dois a seis anos, podendo ser acrescida em um sexto caso o acusado seja funcionário público, além de multa. Também é classificado como crime fazer uso de qualquer documento falsificado ou alterado, a que se referem o art. 297, sujeito as mesmas penalidades (BRASIL, 1940).

Diante disso, com o intuito de inibir fraudes e agilizar a expedição dos documentos, o Ministério da Educação (MEC) publicou, em 5 de abril de 2018, a portaria nº 330 instituindo o diploma digital para instituições de ensino superior, públicas e privadas, pertencentes ao sistema federal de ensino (A portaria completa pode ser visualizada no ANEXO A). De acordo com ela:

> Art. 2º A adoção do meio digital para expedição de diplomas e documentos acadêmicos deverá atender as diretrizes de certificação digital do padrão da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, disciplinado em lei, normatizado e fixado pelo Instituto Nacional de Tecnologia da Informação - ITI, para garantir autenticidade, integridade, confiabilidade, disponibilidade, rastreabilidade e validade jurídica e nacional dos documentos emitidos.(BRASIL, 2018)

Dentre as tecnologias existentes na atualidade que visam garantir a segurança de sistemas e dados sensíveis, temos o conceito de Blockchain, também conhecido como "protocolo da confiança", que visa garantir a segurança descentralizando os dados, ou seja, são bases de registros e dados distribuídos e compartilhados que vão armazenando informações sobre todas as transações que ocorrem em uma determinada rede (FERREIRA et al., 2017). Cada nó na rede guarda as mesmas informações que os demais, se um novo bloco é inserido todos os nós são atualizados para receber os novos dados e, dessa forma, voltarem a conter o mesmo conteúdo. Isso impossibilita que novos dados sejam inseridos ou que blocos sejam modificados sem que isso seja percebido por todos os nós da rede.

A rede de cadeias de blocos também pode ser utilizada para diversos outros propósitos, como comunicações em cadeia de fornecimento, contratos inteligentes, gerenciamento de identidade digital e em uma série de outras aplicações (PILKINGTON, 2016). Por isso, propomos este trabalho com o intuito de conhecer mais como se dá o processo de emissão de diplomas e apresentar uma proposta de solução tecnológica utilizando os conceitos de segurança da rede Blockchain, que têm se mostrado eficientes em diversas outras aplicações, e assim conferir uma maior confiabilidade e segurança ao processo de emissão destes documentos.

1.2 Objetivos

Os principais objetivos deste trabalho são:

1.2.1 Objetivo Geral

Desenvolver uma proposta de aplicação para emissão e validação de diplomas digitais utilizando uma rede Blockchain, buscando atender aos requisitos principais de segurança, conhecidos como tríade CIA, que são confiabilidade, integridade e disponibilidade (STALLINGS, 2015).

1.2.2 Objetivos Específicos

- Fazer um levantamento dos principais passos para a emissão de diplomas acadêmicos;
- Entender como é realizada a verificação de autenticidade dos documentos expedidos;
- Entender os princípios que regem a criação de estruturas de dados baseados na estrutura Blockchain;
- Especificar os requisitos e modelar a aplicação de um sistema para emissão e validação de documentos utilizando os princípios de segurança da Blockchain;
- Analisar e validar os resultados obtidos.

1.3 Metodologia

Quanto à metodologia de pesquisa utilizada neste trabalho utilizamos a classificação de Provdanov e Freitas (2013) para sua elaboração. Assim, quanto à sua natureza este trabalho é classificado como uma pesquisa aplicada pois busca produzir conhecimento para uma aplicação prática, e assim apresentar solução para um problema específico.

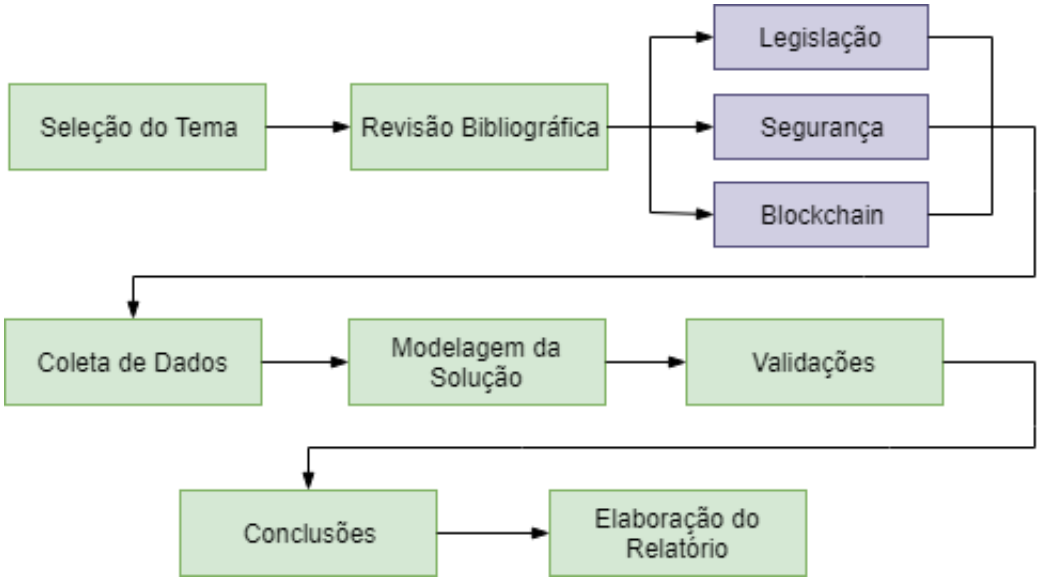
Quanto ao método científico utilizado, é classificado como hipotético-dedutivo, segundo Gil (2008), neste método, dado um problema, são formuladas hipóteses que expressam as dificuldades geradas pelo problema e a partir dessas hipóteses, deduzem-se consequências que serão testadas ou falseadas, ou seja refutadas.

Os objetivos de estudo deste trabalho são classificados como exploratórios, pois visam proporcionar uma maior compreensão sobre um problema e formular hipóteses sobre ele e a abordagem desta pesquisa é qualitativa.

Os procedimentos técnicos utilizados foram a pesquisa bibliográfica, onde buscamos informações em materiais já publicados, realizamos também levantamento de dados através de entrevista e por fim analisamos os resultados obtidos.

As etapas que compõem a metodologia utilizada no trabalho são mostradas de forma esquemática na Figura 1, e em seguida apresentamos o seu detalhamento:

Figura 1 – Estrutura de desenvolvimento do trabalho



Fonte: Próprio autor

Após a definição do tema, iniciou-se a revisão bibliográfica, onde buscamos informações acerca da legislação que regulamenta a emissão de diplomas e certificados, procuramos conhecer mais sobre os mecanismos de segurança empregados atualmente em sistemas distribuídos e pesquisamos também sobre o conceito de Blockchain, suas vantagens e possibilidades de aplicações.

Em seguida realizamos uma coleta de dados através de uma entrevista com servidores da UFRPE, com o intuito de saber como se dá o processo de emissão e validação de diplomas e certificados. E, com base nos estudos realizados e nos dados obtidos, realizamos a modelagem da nossa solução que consiste em um sistema para emissão e validação de diplomas e certificados utilizando os mecanismos de segurança proporcionados pela Blockchain.

Após a modelagem, realizamos a implementação de uma versão inicial do sistema e analisamos a sua consistência e confiabilidade, para assim fazermos a validação do modelo proposto.

1.4 Organização

Uma breve descrição dos conteúdos que compõem cada capítulo deste trabalho é apresentada a seguir:

No capítulo 2 apresentamos a revisão bibliográfica realizada acerca dos temas tratados neste trabalho, como se dá o funcionamento de uma rede Blockchain, como é

feita a geração e validação de um novo bloco e quais são os mecanismos adotadas para garantir a segurança e a integridade dos dados que são registrados. Apresentamos também alguns exemplos de aplicações que utilizam Blockchain como base e pesquisamos como se dá o processo de emissão e validação de um diploma atualmente e quais os mecanismos de segurança são empregados para garantir a segurança dos dados.

No terceiro capítulo detalhamos a nossa implementação, que permite realizar a geração de diplomas digitais e registrá-los em uma rede Blockchain local, o que permitirá consultar com facilidade a autenticidade e integridade dos documentos, podendo-se constatar o momento em que ele foi emitido e gravado no bloco.

No quarto capítulo apresentamos os resultados obtidos, as conclusões e as possibilidades de trabalhos futuros que poderão ser realizados a partir desta pesquisa.

2 Fundamentação Teórica

Neste capítulo serão apresentados conceitos fundamentais para a compreensão desse trabalho. Na seção 2.1 apresentaremos o conceito de Blockchain, como surgiu, quais os princípios de segurança utilizados em seu funcionamento e descreveremos também algumas das inúmeras possibilidades de aplicações que podem ser implementadas com base nessa tecnologia. Na seção 2.2 discorreremos sobre os mecanismos que são utilizados atualmente para conferir segurança a sistemas distribuídos. Na seção 2.3 serão apresentadas informações sobre a forma como se dá a emissão de diplomas atualmente e como será a emissão dos documentos digitais de acordo com a regulamentação do Ministério da Educação.

2.1 Blockchain

O conceito de Blockchain foi definido pela primeira vez em 2008 com a publicação do artigo "Bitcoin: A Peer-to-Peer Electronic Cash System", publicado por uma pessoa ou grupo sob o pseudônimo de Satoshi Nakamoto (cuja real identidade permanece um mistério até os dias de hoje).

Na época o mundo vivia uma grave crise financeira desencadeada pela chamada bolha imobiliária, que gerou desemprego, instabilidade nas bolsas de valores e desconfiança em investidores. Em meio a este cenário a rede Blockchain foi definida para dar suporte a criação da criptomoeda Bitcoin, que teve como objetivo, dentre outras coisas, aumentar a confiança das transações financeiras, levando-as para a internet.

No modelo financeiro tradicional as moedas possuem regulamentações cambiais de bancos ou estados e para que uma transação seja feita é necessário que esta seja confirmada por uma entidade confiável. Para transferirmos dinheiro para outra pessoa temos que pagar algumas taxas ao banco, ou seja, as transações passam obrigatoriamente por um sistema centralizado (PROOF, 2017). As criptomoedas surgiram para contornar todos esses entraves burocráticos, estas não são regulamentadas por nenhum banco ou país e devido a natureza descentralizada da Blockchain as transações são feitas pessoa a pessoa sem a necessidade de uma entidade centralizada para validá-las e cobrar altas taxas por isso.

De acordo com Ferreira et al. (2017) podemos entender Blockchain (também conhecido como protocolo de confiança) como bases de dados distribuídas e criptografadas que funcionam como um livro-razão, que serve para registrar todas as transações que ocorrem em uma determinada rede. Esse registro se dá de forma pública e compartilhada,

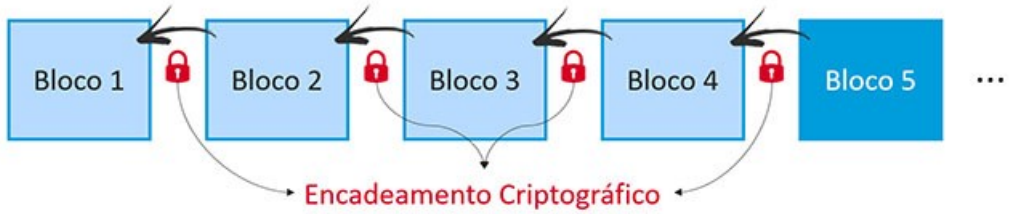
através de protocolos de consenso e confiança entre as partes envolvidas, sem a necessidade do intermédio de terceiros.

2.1.1 Mineração

As transações que ocorrem na rede vão sendo agrupadas e armazenadas em blocos, cada novo bloco precisa ser validado para saber se este atende aos requisitos definidos pela rede. Essa validação, conhecida popularmente como mineração[1], consiste em um custoso procedimento computacional que busca encontrar um *hash*[2] válido para o bloco. O *hash* trata-se de um código composto por números encriptados que serve como um "protocolo" que garante que aquela transação é válida, ao ser encontrado o bloco pode enfim ser adicionado a rede (NAKAMOTO, 2008).

Cada computador (também conhecido como nó) conectado à rede Blockchain guarda uma cópia do "livro-razão", que armazena o registro de todas as transações. Quando um novo bloco é validado e adicionado à rede todos os nós são atualizados para receber os novos valores e assim, garantir a integridade da rede. Isso assegura que novos blocos não possam ser inseridos ou modificados no meio da cadeia sem que isso seja imediatamente percebido pelos demais. Na Figura 2, apresentamos uma representação que como se dá a estruturação da cadeia de blocos.

Figura 2 – Estrutura de organização da rede Blockchain



Fonte: https://www.proof.com.br/blog/blockchain/

O primeiro bloco da cadeia, chamado bloco gênesis, é codificado pelo *software* e serve como o estado inicial do sistema. Ele pode conter informações sobre as regras ou instruções que os demais blocos deverão obedecer. Em 2009, o Bitcoin e a Blockchain foram lançados em código aberto para o mundo, no momento em que Satoshi Nakamoto realizou a mineração do bloco gênesis da cadeia.

2.1.2 Estrutura de um Bloco

De acordo com Ferreira et al. (2017), um bloco é composto por duas partes principais que são o cabeçalho e as transações. As transações são o agrupamento dos dados que

[1] Utilizaremos os termos mineração e validação como sinônimos neste trabalho

[2] Cadeias de caracteres que servem como identificadores de dados que se encontram armazenados em um determinado local

são armazenados no bloco. E o cabeçalho, por sua vez, possui diversos campos, sendo os mais importantes para seu funcionamento: o hash do bloco anterior, dificuldade e nonce, conforme explicaremos posteriormente. Além destes, também é preciso entender dois conceitos importantes: altura do bloco e o hash do cabeçalho, que têm a função de identificar o bloco e sua posição na cadeia, respectivamente. A seguir apresentamos brevemente cada um desses conceitos, de acordo com Ferreira et al. (2017).

- **Transações:** No Bitcoin uma transação é uma transferência de valores. De forma resumida, é um conjunto de endereços de origem dos valores e de endereços de destino para onde os valores serão enviados. Quando um nó cria uma transação, ele a envia aos seus vizinhos e estes, por sua vez, reenviam as demais, até que alcance todos os nós da rede. Quando a transação alcança um nó minerador, ele a guarda para incluir no próximo bloco que será minerado. Quando o bloco for validado e incluído na cadeia, a transação se tornará pública e inalterável.

- **Hash do bloco anterior:** É a existência deste campo, presente no cabeçalho, que permite o encadeamento dos blocos, ligando o bloco atual ao seu anterior e assim sucessivamente. Dessa forma é possível percorrer toda a cadeia até alcançar o bloco gênesis, que por sua vez, possui o campo hash do bloco anterior preenchido com zero, por inexistir blocos anteriores a ele.

- **Nonce:** Consiste em um número usado como variável para alterar o resultado gerado pelo cabeçalho. É utilizado para provar que um minerador realizou trabalho e conseguiu encontrar um hash válido para o bloco, ou seja, que atende aos critérios estabelecidos pela rede.

- **Dificuldade:** A dificuldade é uma colisão parcial de hash. Após o conteúdo das transações serem inseridos em um bloco será gerado o seu hash, pelo processo de mineração. Os algoritmos de hash geram sempre o mesmo resultado caso ocorram entradas iguais, assim depende do poder computacional do nó minerador encontrar um hash que satisfaça essa colisão parcial. Para isso é utilizado o nonce, como ele faz parte do cabeçalho, sempre que for alterado o hash do cabeçalho mudará, logo, encontrar um nonce adequado que satisfaça a dificuldade da rede é uma tarefa que requer alto poder computacional, o que implica em tempo de mineração e consumo de energia.

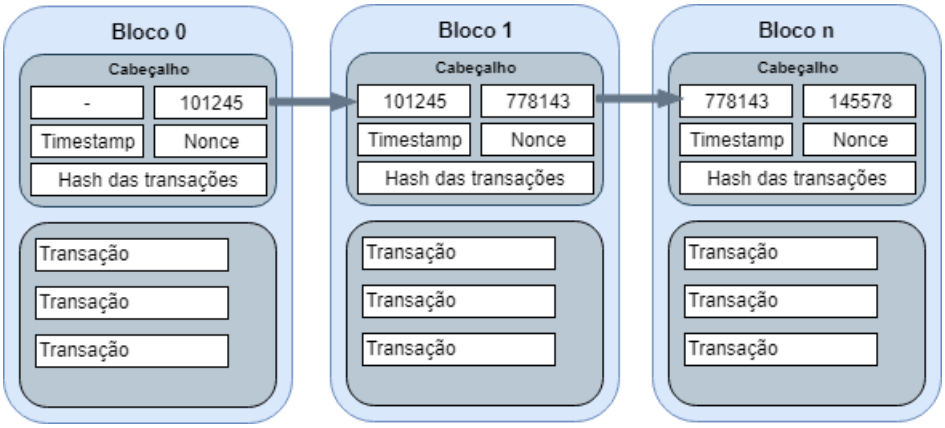
- **Hash do cabeçalho:** É o principal identificador do bloco dentro da cadeia. Após todas as informações terem sido validadas e incluídas no cabeçalho, o hash do cabeçalho é gerado. É ele que é incluído no bloco posterior para garantir o encadeamento dos blocos da rede.

- **Altura do bloco:** Os blocos são incluídos na cadeia de forma sequencial. A diferença entre a posição de um bloco e o bloco gênesis da cadeia é denominada altura do bloco.

- **Timestamp:** Junto a cada bloco da cadeia é armazenado o momento em que ele foi gerado. Este registro se dá através de um número que representa a quantidade de segundos decorridos entre o momento em que o bloco foi gerado e o dia 01 de janeiro de 1970.

Na Figura 3, apresentamos uma representação mais detalhada da estrutura dos blocos e dos principais campos contidos neles.

Figura 3 – Estruturas dos bloco da Blockchain



Fonte: O autor

No retângulo inferior de cada bloco na figura estão as transações que vão sendo adicionadas uma a uma até que o limite do bloco seja atingido. No retângulo superior dos blocos está a representação do cabeçalho, contendo o hash das transações, o hash do bloco anterior, o hash do bloco que é o seu identificador, é ele que é enviado ao bloco seguinte, também o *timestamp* registrando o momento em que aquele bloco foi gerado e o nonce que é utilizado para a validação do bloco.

2.1.3 Aplicabilidade da Blockchain

Como dito anteriormente, a Blockchain surgiu para dar suporte a rede de criptomoedas Bitcoin. No entanto devido a sua natureza descentralizada e a segurança conferida pelo sua maneira de registrar informações logo surgiram inúmeras outras aplicabilidades possíveis para ele (TEIXEIRA; TAVARES, 2018). A seguir apresentamos brevemente algumas dessas aplicabilidades.

2.1.3.1 Internet das Coisas

A Internet das Coisas - IoT (do inglês Internet of Things) é um conceito relativamente novo, que tem como principal objetivo dar a objetos simples, do dia a dia, capacidade computacional e conectá-los à Internet. Segundo Ferreira et al. (2017), a IoT abrange o processamento de dados e a comunicação entre diferentes dispositivos de forma autonômica, sem intervenção humana.

De acordo com Balte, Kashid e Patil (2015), com o uso da IoT não se faz mais necessário sentar em um lugar para acessar dispositivos com acesso à Internet; em vez disso a Internet poderá ser acessada de qualquer lugar e de qualquer dispositivo. Isso transformará a realidade das pessoas e sua forma de se relacionar com os objetos do ambiente à sua volta, gerando conforto, comodidade e muito mais praticidade na realização de tarefas dos mais variados tipos.

A quantidade de dispositivos de IoT existentes vem crescendo de maneira rápida e consequentemente o tráfego de dados entre eles também aumenta de forma significativa. Segundo Diego, Papapanagiotou e Yang (2018), em 2020 já existirão cerca de 20 bilhões de dispositivos conectados e a troca de dados entre eles será de mais de 40 Zettabytes. Diante disso, faz-se extremamente necessário garantir a segurança e a privacidade dos dados que são gerados por estes sistemas, os dispositivos da IoT exigem o seguinte conjunto de requisitos de segurança para serem considerados seguros (DIEGO; PAPAPANAGIOTOU; YANG, 2018):

- autenticação segura;
- transmissão segura de dados;
- segurança dos dados utilizados pelos dispositivos de IoT;
- acesso seguro aos dados por pessoas autorizadas;
- protocolos de autenticação.

No contexto da Internet das Coisas, a rede Blockchain pode ser utilizada para autenticar, autorizar e auditar os dados gerados pelos dispositivos e devido a sua natureza descentralizada não há a necessidade de confiança em terceiros e o risco de falhas no sistema é menor (FERREIRA et al., 2017).

2.1.3.2 *Smart Contracts*

Podemos descrever *Smart Contracts* como um código computacional capaz de facilitar, executar e forçar o cumprimento de um acordo, por meio da Blockchain (TECHNOLOGIES, 2018), de forma automática e segura. Tem como principal objetivo permitir

que duas partes, que não precisam se conhecer, façam negócios entre si, normalmente via internet, sem que haja a necessidade de uma entidade centralizada como intermediária.

A ideia de *Smart Contracts* surgiu na década de 90, antes mesmo da existência do Bitcoin, quando Szabo (1994), apresentou a ideia de utilizar softwares para executar contratos. Os contratos inteligentes recebem como entrada uma série de condições, que ficam sendo verificadas e ao serem satisfeitas o contrato se autoexecuta. Toda o processo é automatizado e pode se dar de maneira totalmente virtual ou mista, como um complemento a contratos feitos no papel. A segurança da transação é garantida pela Blockchain.

De acordo com Teixeira e Tavares (2018), o funcionamento dos *Smart Contracts* é divido em três etapas, as quais apresentamos abaixo:

- **Codificação:** Inicialmente é realizada a codificação do contrato em alguma linguagem de programação, no código são definidas com exatidão as instruções que o contrato deve executar e que evidentemente devem estar de acordo com o interesse das partes. O contrato comporta-se da maneira como foi definido sem as nuances linguísticas dos idiomas humanos que abrem margem a dúbias interpretações.

- **Envio à Blockchain:** Após a codificação o código é criptografado e enviado para outros computadores por meio da Blockchain, de forma semelhante ao que é realizado nas transações de Bitcoin.

- **Execução:** Alguns computadores da rede Blockchain recebem o código e o executam, em seguida a rede atualiza os registros para constar os resultados das execuções do contrato e então monitora para conferir se estes estão em conformidade com os termos definidos no *Smart Contracts*.

Este tipo de contrato oferece um alto nível de confiabilidade e segurança, pois não há como controlar a execução do código, já que este se dá de maneira distribuída e descentralizada, também não é possível alterar os resultados da execução, porque elas estão gravadas indelevelmente nos blocos da Blockchain.

2.1.3.3 Registros de autenticidade

A Blockchain, dentre outras coisas, utilizada para a realização do registro de documentos dos mais diversos tipos, atualmente este serviço, também conhecido como BitRegistro, já é utilizado por empresas e cartórios como um mecanismo para assegurar a autenticidade dos seus documentos.

Qualquer documento digital pode ter sua existência comprovada através de um carimbo de tempo fornecido por uma Blockchain pública (ORIGINALMY, 2017). Diversos

tipos de conteúdos podem ser registrados, como obras de arte, declarações, propostas, relatórios e qualquer outro tipo de documento.

No Brasil, uma empresa tem se destacado na utilização de Blockchain para a implementação de diversas soluções tecnológicas: a Originalmy, criada em 2015, foi a primeira empresa brasileira a utilizar Blockchain como protocolo no país, inicialmente com o intuito de realizar autenticação de documentos (ORIGINALMY, 2017). Atualmente outros serviços foram incorporados à plataforma, como:

- **Prova de autenticidade para conteúdo web:** Utilizando um plugin no navegador, permite comprovar que um determinado conteúdo estava online em um dado momento, o que pode ser muito útil como prova em situações de calúnia e difamação em redes sociais.
- **Assinatura de Contratos:** Permite o registro de contratos no Blockchain, garantindo sua autenticidade através de uma assinatura digital. A plataforma notifica aos interessados caso haja um novo contrato disponível precisando ser assinado.
- **Identidade Blockchain** Ao se cadastrar, o sistema cria uma Identidade Blockchain que fica em posse do usuário. Através dessa identidade única e exclusiva, o usuário pode efetuar ações na plataforma.

2.2 Segurança da Informação

Nos dias de hoje, cresce cada vez mais a preocupação das pessoas e empresas com relação à segurança da informação, para muitas corporações, a informação pode ser considerada um produto de altíssima importância, sua manipulação indevida pode ocasionar inúmeros prejuízos, por isso muitos cuidados precisam ser tomados, principalmente com relação aos meios de armazenamento e divulgação utilizados (GULO, 2012).

2.2.1 Princípios de segurança

Para que um sistema seja considerado seguro ele precisa atender a alguns princípios, que segundo Stallings (2015) são integridade, disponibilidade e confiabilidade. Conforme descrevemos a seguir:

- **Integridade:** Busca assegurar que as informações armazenadas em um sistema sejam modificadas somente de uma maneira especificada e autorizada.
- **Disponibilidade:** Este princípio busca garantir que um sistema esteja sempre pronto para realizar as tarefas as quais se destina

- **Confiabilidade:** Deve assegurar que somente indivíduos autorizados tenham acesso as informações e realizem alguma modificação sobre elas.

Para Ferreira et al. (2017) é possível obter segurança usando uma combinação de mecanismos de autenticação, autorização e identificação. Com isto podemos verificar a identidade de quem deseja realizar uma determinada função em um sistema e verificar quais direitos esse usuário possui. Outro ponto importante que deve ser levado em consideração é a necessidade de armazenar informações de uso de cada usuário, isso para garantir que ele não negue ter realizado determinada ação, este princípio é conhecido como não repúdio e fornece provas de tudo o que ocorreu no sistema.

2.2.2 Uso de Blockchain para atender aos princípios de segurança

É possível fazer uso do Blockchain para implementar todos os princípios de segurança mencionados anteriormente. Com o registro na cadeia de blocos podemos assegurar o principio da integridade, pois as informações contidas nas transações não podem ser modificadas intencionalmente por indivíduos maliciosos, nem serem afetadas por eventos futuros, como surtos de energia ou falhas em um banco de dados, já que os dados estão replicados por toda a extensão da rede.

A descentralização da rede garante também a constante disponibilidade dos dados, mesmo que determinados nós fiquem temporariamente inoperantes, por quaisquer que sejam os motivos, a rede continuará disponível pois as informações poderão ser acessadas a partir das diversas outras cópias existentes.

Na Blockchain os usuários são identificados através de um mecanismo de pseudo anonimato, através de endereços criptografados que são resumos de suas chaves públicas, isso proporciona o princípio da confidencialidade, pois somente indivíduos registrados podem ter acesso as informações do sistema.

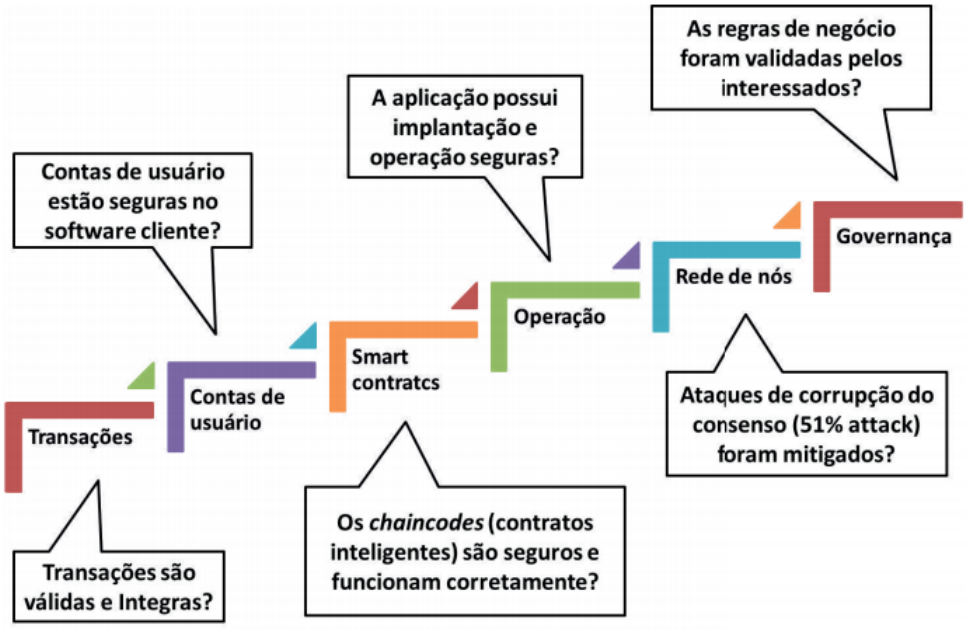
De acordo com Braga, Marino e Santos (2017) as aplicações construídas sobre Blockchain devem ser estruturadas em seis camadas de segurança, que são descritas adiante e ilustradas na Figura 4.

- **Segurança da transação:** É a primeira camada e a mais básica de todas: a Blockchain deve validar as transações com confiança e previsibilidade utilizando os consensos da rede.

- **Segurança da conta de usuário:** Os próprios usuários devem gerenciar suas contas, fazendo uso de carteiras digitais (*eWallets*).

- **Segurança da aplicação e dos contratos:** Nesta camada são definidos mecanismos de segurança que serão utilizados no desenvolvimento dos softwares de geração dos *smart contracts*.
- **Segurança de implantação e de operação da aplicação:** Aqui são inclusos os testes de aceitação da aplicação antes da sua implantação. Uma vez no ambiente de produção, a aplicação deve ser constantemente monitorada para detecção de possíveis anomalias de funcionamento.
- **Segurança da rede P2P de seus nós:** Nesta camada são implementados os mecanismos tradicionais de segurança de redes, como *firewall*, IDS, IPS, etc, para proteger os nós da rede P2P Blockchain.
- **Governança da aplicação e da Blockchain:** Por fim, temos as decisões que deverão ser tomadas sobre a arquitetura e o projeto da Blockchain, estas decisões afetarão o funcionamento da rede e a segurança que ela oferecerá.

Figura 4 – Camadas de segurança da Blockchain



Fonte: Braga, Marino e Santos (2017)

Na Figura 4, mostrada acima, podemos ver uma representação das camadas de segurança que são utilizadas na Blockchain. A ilustração é feita em níveis crescentes, começando pela operação mais básica realizada pela rede, que é a validação das transações e inclusão de novos blocos, até chegar na camada superior, que contempla as regras de negócio que devem ser levadas em consideração para que a aplicação cumpra a finalidade a qual se destina. Nos níveis intermediários estão outros mecanismos de segurança adotados, que também são de extrema importância para a eficiência das aplicações, como o registro

seguro das contas de usuário, a implementação segura do código e a capacidade de tolerar possíveis ataques que possam ocorrer contra a rede.

2.3 Diplomas

No Brasil, ao concluir um curso superior em uma instituição de ensino o aluno tem o direito de receber um diploma, que consistem em um documento comprobatório da formação recebida e que lhe confere autorização para exercer a sua profissão em todo o território nacional.

2.3.1 Expedição de diplomas

Para que uma Instituição de Ensino Superior (IES) possa realizar a emissão de diplomas, faz-se necessário que o respectivo curso seja reconhecido pelo Ministério da Educação (MEC) (BRASIL, 1996). Para que haja tal reconhecimento, a IES deverá, após o início do seu funcionamento, protocolar pedido junto ao MEC no período compreendido entre a metade do prazo previsto para a integralização de sua carga horária e setenta e cinco por cento deste prazo, conforme disposto no art. 46 do Decreto nº 9.235/2017. (BRASIL, 2017)

Ao emitir um certificado ou diploma, cabe à IES assegurar a sua regularidade, pois uma vez emitido, presume-se a sua validade conforme o disposto na legislação. Caso haja alguma irregularidade a IES que realizou a emissão sujeitar-se-á às sansões legais aplicáveis. (BRASIL, 2013).

2.3.2 Registro de diplomas

O registro de um diploma representa a validação de que o aluno cumpriu tudo o que era necessário para receber o título referente ao curso superior de que participou. Caso a IES seja uma Universidade ou Centro Universitário deverá ela mesma realizar este registro, caso se trate de uma Faculdade o registro deverá ser feito, obrigatoriamente, por uma instituição credenciada, como uma Universidade pública ou privada. (BRASIL, 2013).

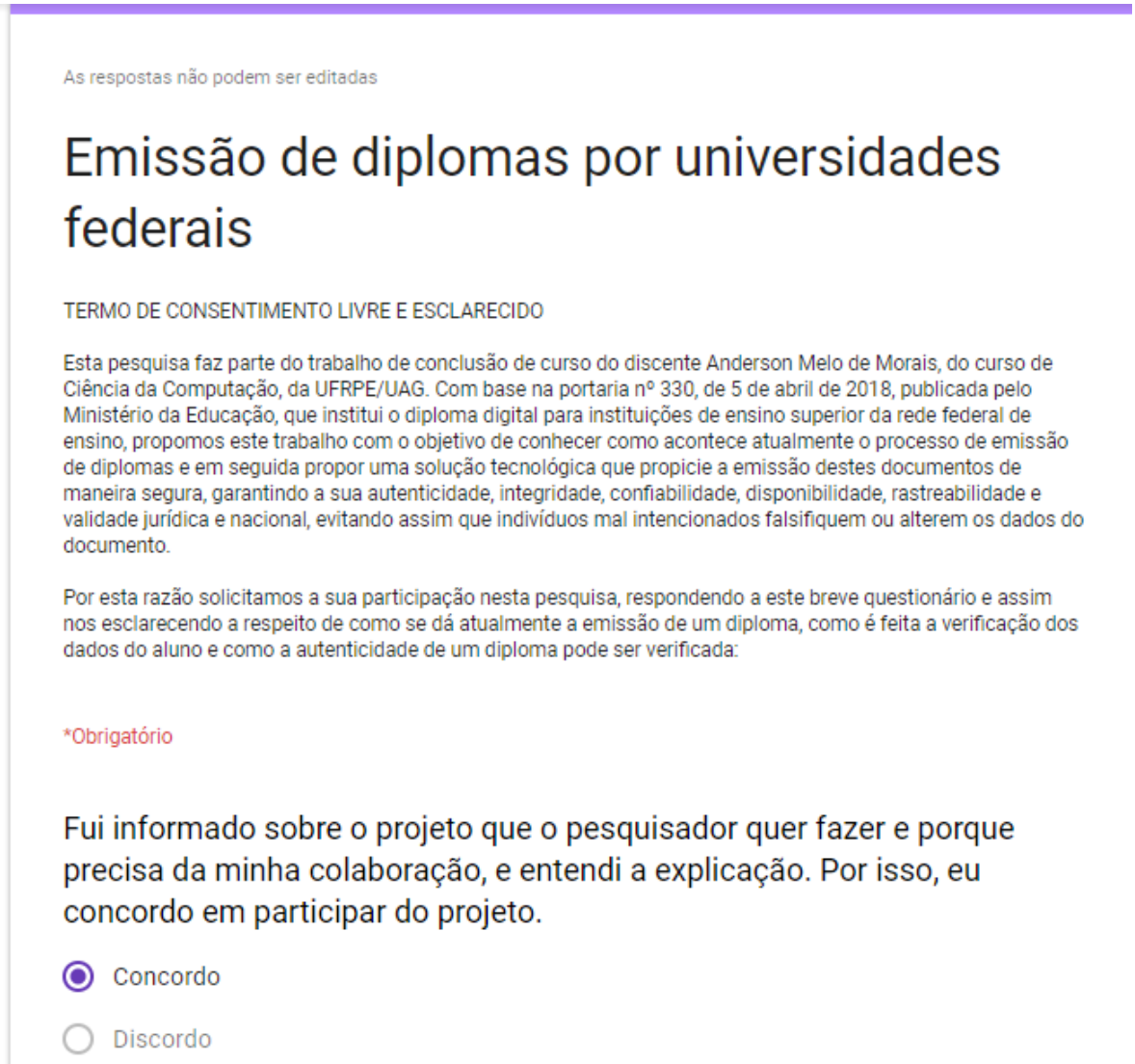
Caso uma IES seja descredenciada pelo MEC, está ainda terá que cumprir com suas obrigações educacionais, ou seja, ainda deverá organizar e manter acervo acadêmico e emitir diplomas e certificados referentes aos cursos que ofertou, desde que tais cursos tenham sido reconhecidos. Ao final do processo de descredenciamento será designada uma nova instituição para realizar a guarda do acervo da instituição desativada.

2.3.3 Entrevista realizada

Com o objetivo de entender melhor como se dá o processo de emissão e validação de um diploma por uma universidade federal, elaboramos uma breve entrevista por meio de um formulário eletrônico e enviamos por e-mail ao departamento de registro e controle acadêmico (DRCA) da UFRPE, que é o departamento responsável pela emissão dos diplomas da referida universidade.

Obtivemos uma resposta, de um servidor do departamento que não autorizou a divulgação do seu nome, nem do cargo exercido na instituição. No início do questionário apresentamos um Termo de Consentimento Livre e Esclarecido (TCLE), onde era explicado o objetivo da pesquisa e pedia que o voluntário concordasse antes de prosseguir para as perguntas seguintes. Na Figura 5, apresentamos o TCLE da pesquisa.

Figura 5 – Termo de Consentimento Livre e Esclarecido da pesquisa

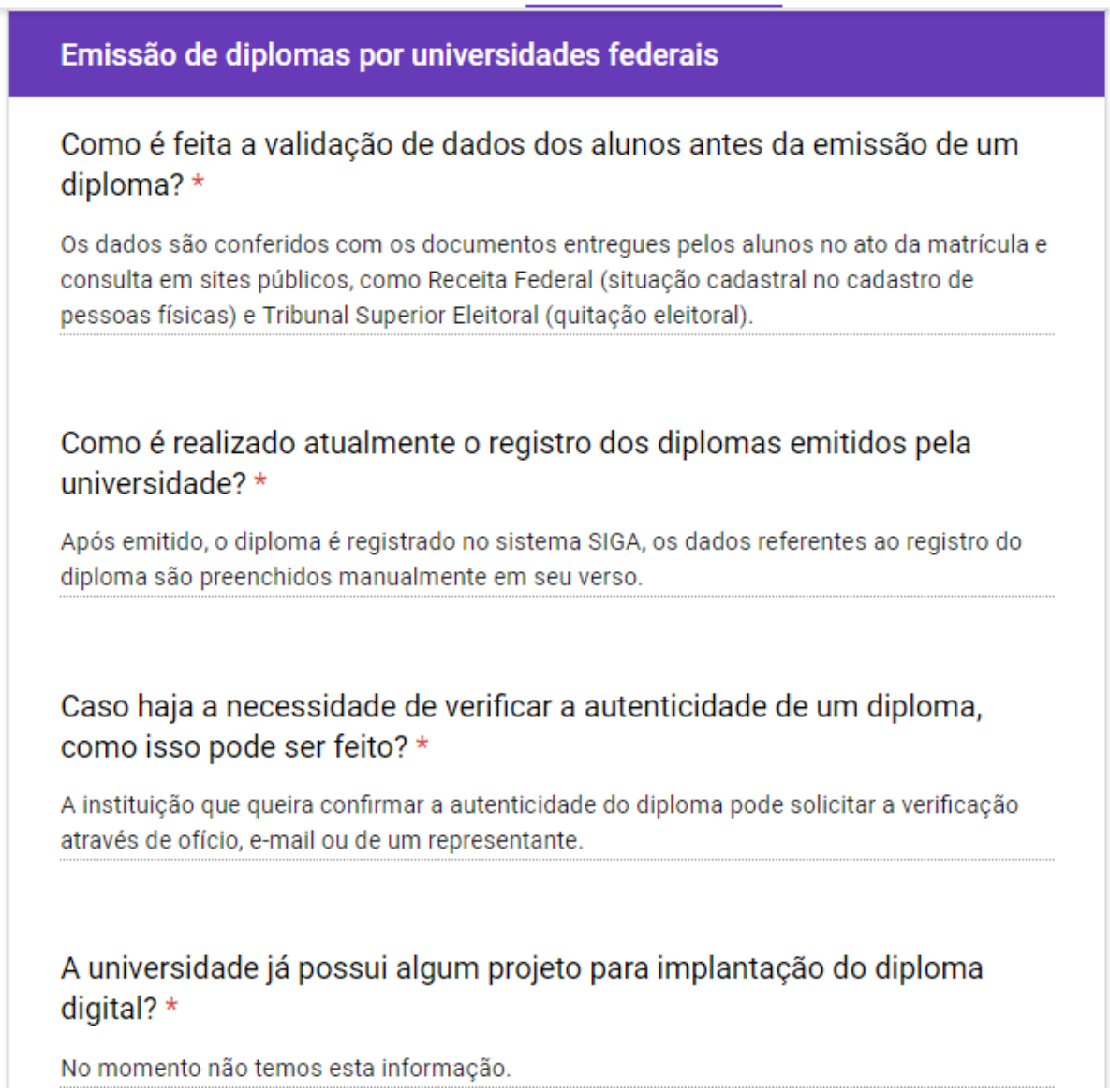


Fonte: O Autor

Na Figura 6, apresentamos as perguntas que foram elaboradas para a entrevista,

bem como as respostas que foram obtidas para cada uma delas.

Figura 6 – Respostas ao formulário de pesquisa



Fonte: O Autor

Como podemos perceber pelas respostas apresentadas ao questionário acima, a maior parte do processo de emissão, registro e validação de um diploma atualmente, acontece de maneira manual.

2.3.4 Diplomas Digitais

No dia 05 de abril de 2018, o Ministério da Educação publicou no Diário Oficial da União, a portaria nº 330 instituindo o diploma digital para todas as instituições de ensino públicas e privadas pertencentes ao sistema federal de ensino (BRASIL, 2018). As instituições terão dois anos para se adequarem à nova medida. De acordo com essa publicação, o diploma digital abrange o registro e o respectivo histórico escolar do aluno.

Sua emissão será feita por Universidades credenciadas e que já são aptas a emitir tais documentos de acordo com a legislação vigente. As universidades que desejarem poderão continuar emitindo os documentos também em papel, desde que haja uma versão digital.

O Art. 2º determina que a emissão do diploma digital deverá atender as diretrizes de certificação digital do padrão da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, que é normatizado e fixado pelo Instituto Nacional de Tecnologia da Informação (ITI). O objetivo da medida é inibir fraudes e agilizar a expedição dos documentos.

2.3.5 ICP-Brasil

De acordo com o Instituto Nacional de Tecnologia da Informação (ITI), a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) consiste em uma cadeia hierárquica de confiança que tem como objetivo viabilizar a emissão de certificados digitais para identificação virtual dos cidadãos (ITI, 2017).

O MEC estabeleceu a obrigatoriedade do uso do certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira para assinatura dos diplomas digitais, com o objetivo de garantir a autenticidade, integridade, confiabilidade, disponibilidade, rastreabilidade e validade jurídica dos documentos emitidos (ITI, 2018).

O intuito da implementação do diploma digital é eliminar as fraudes que ocorrem no processo de emissão de diplomas e tornar o processo mais rápido e transparente.

3 Implementação do Sistema

Neste capítulo, apresentaremos a implementação de uma aplicação que exemplificará o processo de geração de um diploma digital e como se dará a sua inclusão em uma Blockchain local. Na seção 3.1, descreveremos os requisitos, funcionais e não funcionais, que serão necessários para o bom funcionamento do sistema. Na seção 3.2, será apresentada a prototipação do sistema, onde mostraremos as principais telas da aplicação e as funcionalidades inerentes a cada uma delas. Na seção 3.3, mostraremos como se dá o funcionamento da rede Blockchain local utilizada neste projeto.

3.1 Definição dos requisitos

A fase inicial na elaboração de um projeto de *software*, e uma das mais importantes para o bom êxito das demais, é a Engenharia de Requisitos, pois esta fornece mecanismos apropriados para compreendermos qual problema o sistema deve resolver, quais necessidades ele deve atender, e assim, podermos avaliar as possíveis formas de solução, validando a especificação e gerindo os requisitos (PRESSMAN, 2009). Nesta seção apresentaremos os requisitos funcionais e não funcionais deste projeto.

3.1.1 Requisitos funcionais

Requisitos funcionais (RF), são aqueles que definem recursos específicos do sistema, as funções de um sistema e seu componentes, podendo ser cálculos, comportamentos, manipulação de dados dentre outras. Na Tabela 1, apresentamos os RF da aplicação que denotam as principais funcionalidades que devem ser apresentadas.

Tabela 1 – Requisitos Funcionais

ID	Nome	Prioridade
RF 01	Consulta de alunos	Essencial
RF 02	Geração do diploma	Essencial
RF 03	Registro do diploma na Blockchain	Essencial
RF 04	Registro do diploma no base de dados	Essencial
RF 05	Validação dos diplomas	Essencial

Na tabela acima podemos ver os requisitos funcionais essenciais da aplicação, que consistem na busca do aluno na base de dados, mediante a informação do seu número de CPF, geração do seu respectivo diploma no formato PDF, inserção da hash do diploma gerado na Blockchain local e também na base de dados para eventuais consultas posteriores e por fim, a validação de um documento emitido, que consistirá em submetê-lo novamente

ao sistema, calcular o seu hash e verificar se este se encontra registrado na Blockchain e na base de dados da aplicação.

Na coluna ID ao lado esquerdo da tabela listamos os RF de forma sequencial e na coluna Prioridade, ao lado direito, indicamos o grau de prioridade com que cada RF deve ser tratado, como podemos ver todos são assinalados com Essencial, por se tratarem das principais funcionalidades inerentes a aplicação proposta.

3.1.2 Requisitos Não-Funcionais

Requisitos Não-Funcionais (RNF) são aqueles que dizem respeito ao uso do sistema em termos de desempenho, usabilidade, confiabilidade, segurança dentre outros, podendo estes, se não observados da forma correta, causar o mau funcionamento do sistema ou até sua inutilização (SOMMERVILLE, 2007). Na Tabela 2, mostramos alguns requisitos não funcionais da aplicação.

Tabela 2 – Requisitos Não-Funcionais

ID	Nome	Prioridade
RNF 01	Segurança dos dados	Essencial
RNF 02	Design responsivo	Desejável
RNF 03	Escalabilidade da aplicação	Essencial
RNF 04	Divisão arquitetural em camadas	Essencial
RNF 05	Facilidade de aprendizagem e recordação	Desejável

De forma análoga ao apresentado anteriormente temos que a tabela acima é organizada de forma sequencial, como indicado pela coluna ID do lado esquerdo, e também indicamos a prioridade de cada RNF da aplicação, como descrito na coluna Prioridade ao lado direito.

Alguns requisitos são assinalados como essenciais, por serem de extrema importância para o contexto do sistema. Os dados precisam ser armazenados de maneira segura, podendo ser acessados apenas por indivíduos autorizados, a aplicação deve ser escalável permitindo que um grande número de requisições sejam atendidas em tempo hábil e o sistema será dividido em camadas para facilitar a sua manutenção, aumentando assim a coesão e reduzindo o acoplamento.

Outros requisitos são tidos como desejáveis, apesar de não serem essenciais para o funcionamento da aplicação, contribuem para uma boa experiência do usuário, como possuir um design responsivo e apresentar facilidade de aprendizado e recordação.

3.2 Prototipação

Após a definição dos requisitos do sistema, realizamos a implementação de algumas de suas funcionalidades principais. Nesta seção, descreveremos as ferramentas utilizadas para o desenvolvimento e mostraremos, por meio de imagens, os resultados obtidos.

3.2.1 Ferramentas utilizadas

A seguir apresentamos as principais ferramentas utilizadas para o desenvolvimento da aplicação.

- **Node.js:** Para o desenvolvimento da aplicação escolhemos a plataforma Node.js, devido à boa performance e o alto desempenho oferecido por ela.
- **HTML5/CSS3:** Para o front-end da aplicação, utilizamos HTML5 e CSS3, com o objetivo de conferir-lhe uma boa aparência e proporcionar uma boa experiência de usabilidade ao usuário.
- **MongoDB:** Para a base de dados utilizamos o MongoDb, que é um banco de dados NoSQL e apresenta um modelo de dados flexível que permite o fácil crescimento e evolução da aplicação.
- **Docker:** Para a simulação da rede Blockchain local necessitamos criar nós, ou máquinas virtuais, para isso, utilizamos o Docker que permite a instanciação de serviços de maneira eficiente e sem demandar muitos recursos computacionais.
- **GIT:** Para uma melhor organização do código e para controle de versões, utilizamos o GIT e criamos um repositório na plataforma GitHub.
- **Sublime Text:** Como editor de texto utilizamos o Sublime Text 3, pois o mesmo permite a visualização dos arquivos e diretórios do projeto de maneira simples e prática.

3.2.2 Detalhes da aplicação

Na Figura 7, podemos visualizar a interface da tela de login da aplicação. Nela é possível inserir um nome de usuário e uma senha para que se possa ter acesso ao sistema. São realizadas tratativas para impedir que o usuário tente realizar login deixando um dos campos em branco, caso ele tente, uma mensagem de alerta é exibida. Ao clicar no botão "Entrar", mostrado no canto inferior direito, a aplicação criptografa a senha informada utilizando o módulo Crypto, disponível no Node.js, e compara com o valor que se encontra cadastrado no banco, caso as senhas sejam iguais, o usuário é autorizado a acessar a aplicação.

Figura 7 – Imagem da tela de login da aplicação

Fonte: O Autor

No Código 3.1, apresentamos um trecho do código da aplicação utilizado para a realização do login do usuário. Nele é feita a utilização do módulo Crypto, na linha 5, e em seguida é realizada uma consulta no banco para verificar se o usuário se encontra cadastrado, linhas de 10 a 20.

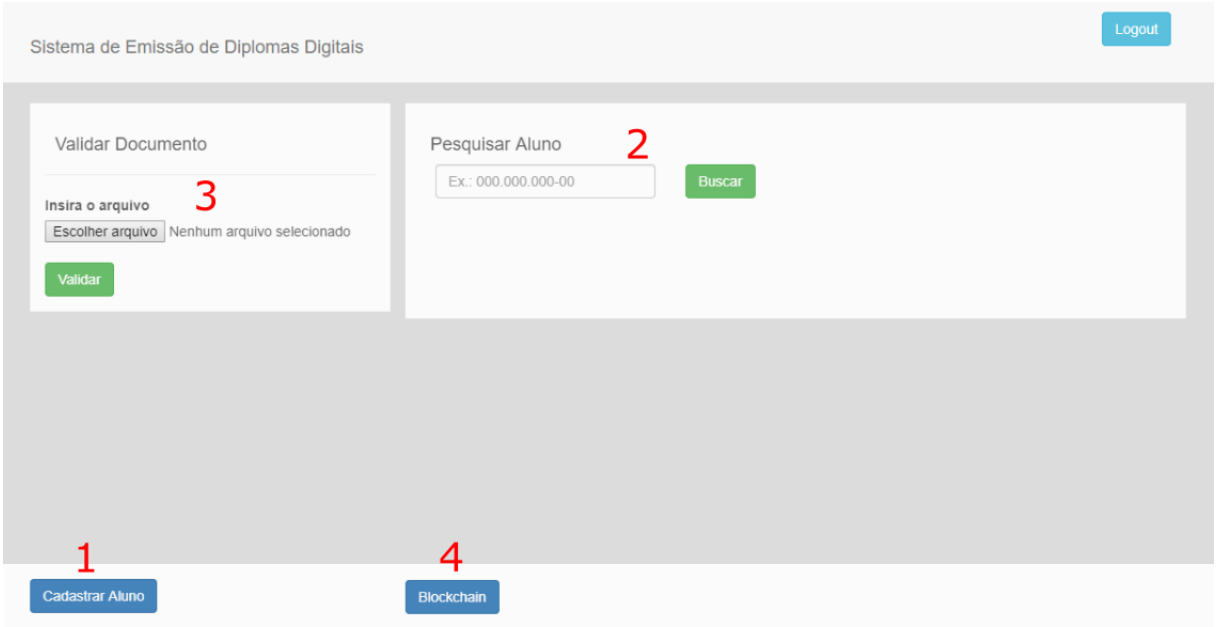
Código 3.1 – Código da tela de login

```
1  UsuariosDAO.prototype.autenticar = function(usuario, req, res){
2    this._connection.open( function(err, mongoclient){
3      mongoclient.collection("usuarios", function(err, collection){
4
5        var senha_criptografada = crypto.createHash("sha256").
6        update(usuario.senha).digest("hex");
7
8        usuario.senha = senha_criptografada;
9
10       collection.find(usuario).toArray(function(err, result){
11         if(result[0] != undefined){
12           req.session.autorizado = true;
13           req.session.usuario = result[0].usuario;
14         }
15         if(req.session.autorizado){
16           res.redirect("home");
17         }else{
18           res.render("index", {validacao: {}});
19         }
20       });
21       mongoclient.close();
22     });
23   });
```

```
24 }
```

Ao realizar o login o usuário é redirecionado para a página inicial, como podemos observar na Figura 8, onde ele tem acesso as principais funcionalidades disponibilizadas pelo sistema, como o cadastro de um novo aluno, indicado na Figura com 1, a busca por um aluno já cadastrado na base, destacado com o número 2, a validação de um diploma já emitido, indicado pelo 3 e a visualização dos dados da Blockchain, apresentado na figura com o número 4.

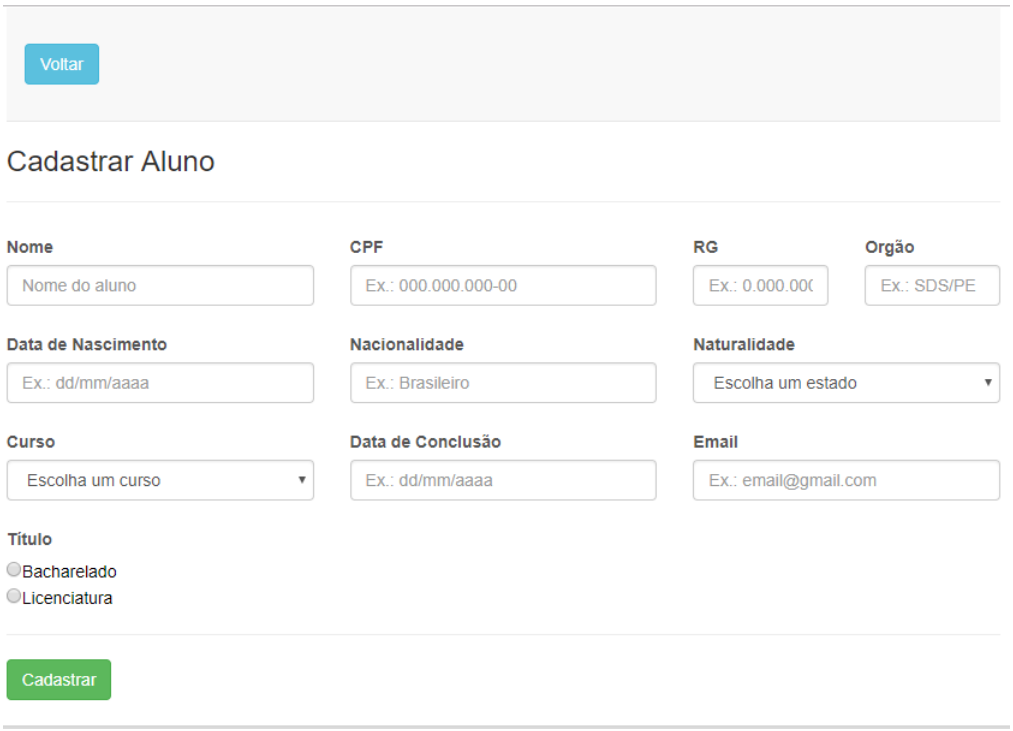
Figura 8 – Imagem da tela inicial da aplicação



Fonte: O Autor

Para o exemplo da aplicação proposta neste trabalho desconsideramos a existência de uma base de dados que já contenha todos os dados dos alunos da instituição, o que certamente aconteceria em um cenário real, assim incluímos um botão "Cadastrar Aluno"na tela inicial que ao ser clicado redireciona o usuário para a tela mostrada na Figura 9, onde é possível inserir os principais dados de um aluno (como nome, curso, números de documentos, etc.), que serão exibidos em seu diploma no momento em que este for gerado.

Figura 9 – Tela de cadastro de novo aluno



Fonte: O Autor

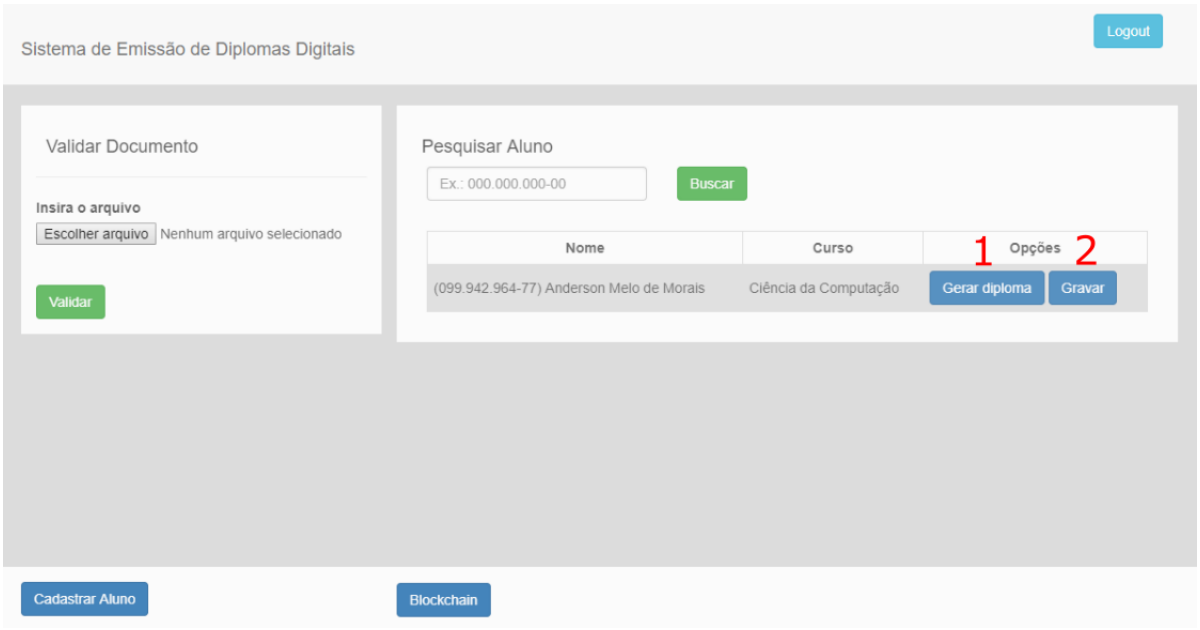
No Código 3.2, apresentamos um trecho do código responsável pelo cadastro de um novo aluno. Ele realiza a conexão com o banco de dados MongoDB e utiliza o método *insert* que é nativo do mongo, para a inserção, como mostrado nas linhas de 3 a 11.

Código 3.2 – Código de cadastro de um novo aluno

```
1  UsuariosDAO.prototype.inserirUsuario = function(usuario){
2
3    this._connection.open( function(err, mongoclient){
4      mongoclient.collection("aluno", function(err, collection){
5
6        nome = usuario.nome.toLowerCase().split(" ");
7        usuario.tags = nome;
8        collection.insert(usuario);
9        mongoclient.close();
10     });
11   });
12 }
```

A busca por um aluno pode ser realizada mediante a inserção do seu CPF no campo indicado no centro da tela inicial, ao clicar no botão "buscar"o sistema exibirá o resultado da consulta, contendo o CPF, o nome e o curso do aluno, ao lado direito dessas informações dois botões que permitem ao usuário gerar o diploma do aluno e grava-lo na Blockchain. Na Figura 10 mostramos um exemplo de consulta realizada no sistema, com os dados do aluno sendo exibidos na tela.

Figura 10 – Imagem da realização da uma busca de um aluno no sistema



Fonte: O Autor

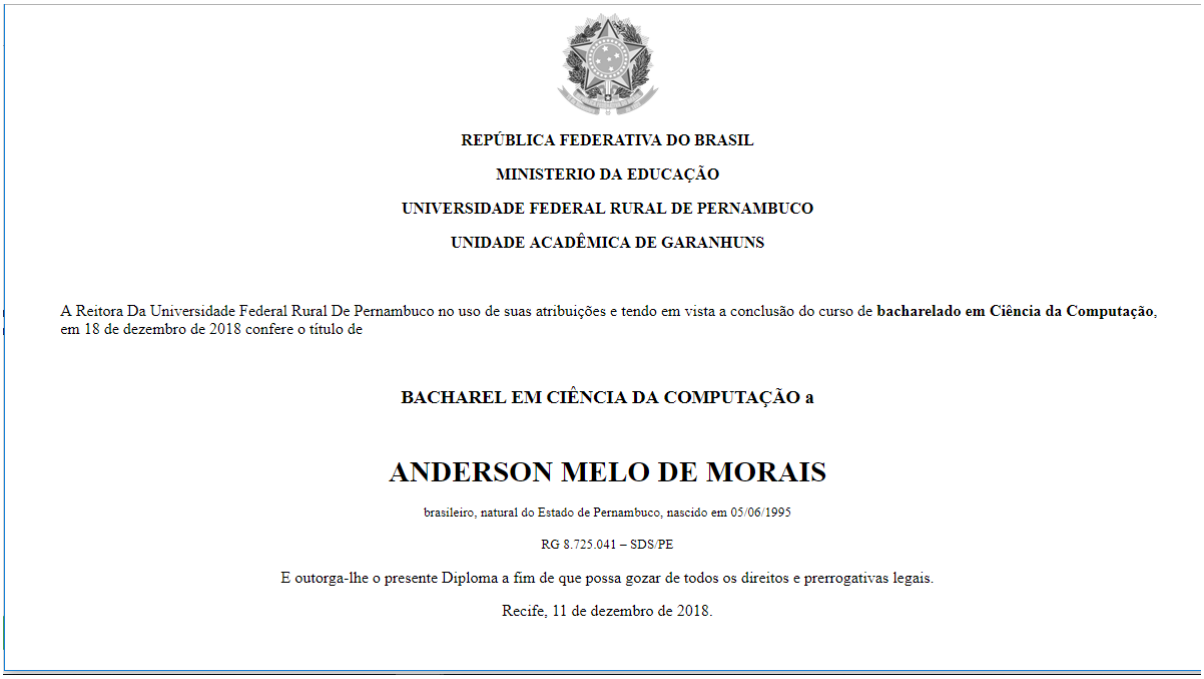
No Código 3.3, podemos ver como é feita a busca de um aluno, este realiza uma conexão com o banco de dados e, utilizando a função *find* que é nativa do mongo, busca pelo aluno na base, passando como parâmetro o CPF informado pelo usuário, como podemos visualizar nas linhas de 2 a 13.

Código 3.3 – Código que realiza a busca por um aluno

```
1  DiplomaDAO.prototype.getAlunos = function(usuario, res) {
2    this._connection.open( function(err, mongoclient){
3      mongoclient.collection("aluno", function(err, collection){
4
5        search = usuario.cpf;
6
7        collection.find({cpf : search}).toArray(function(err, result){
8          res.render("pesquisa", {acoes: result});
9        });
10
11       mongoclient.close();
12     });
13   });
14 }
```

Ao clicar no botão gerar diploma, destacado na Figura 10 com o número 1, a aplicação exibirá uma página com o modelo de um diploma preenchido com os dados do respectivo aluno, conforme mostrado na Figura 11.

Figura 11 – Representação de um dos diplomas gerados pola aplicação



REPÚBLICA FEDERATIVA DO BRASIL

MINISTERIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

UNIDADE ACADÊMICA DE GARANHUNS

A Reitora Da Universidade Federal Rural De Pernambuco no uso de suas atribuições e tendo em vista a conclusão do curso de **bacharelado em Ciência da Computação**, em 18 de dezembro de 2018 confere o título de

BACHAREL EM CIÊNCIA DA COMPUTAÇÃO a

ANDERSON MELO DE MORAIS

brasileiro, natural do Estado de Pernambuco, nascido em 05/06/1995

RG 8.725.041 – SDS/PE

E outorga-lhe o presente Diploma a fim de que possa gozar de todos os direitos e prerrogativas legais.

Recife, 11 de dezembro de 2018.

Fonte: O Autor

Ainda na tela de busca, ao lado dos dados do aluno, encontramos um botão "Gravar", destacado com o número 2 na Figura 10, que ao ser clicado verifica se o diploma já se encontra salvo no formato PDF, em caso positivo o hash deste arquivo é calculado e inserido no Blockchain.

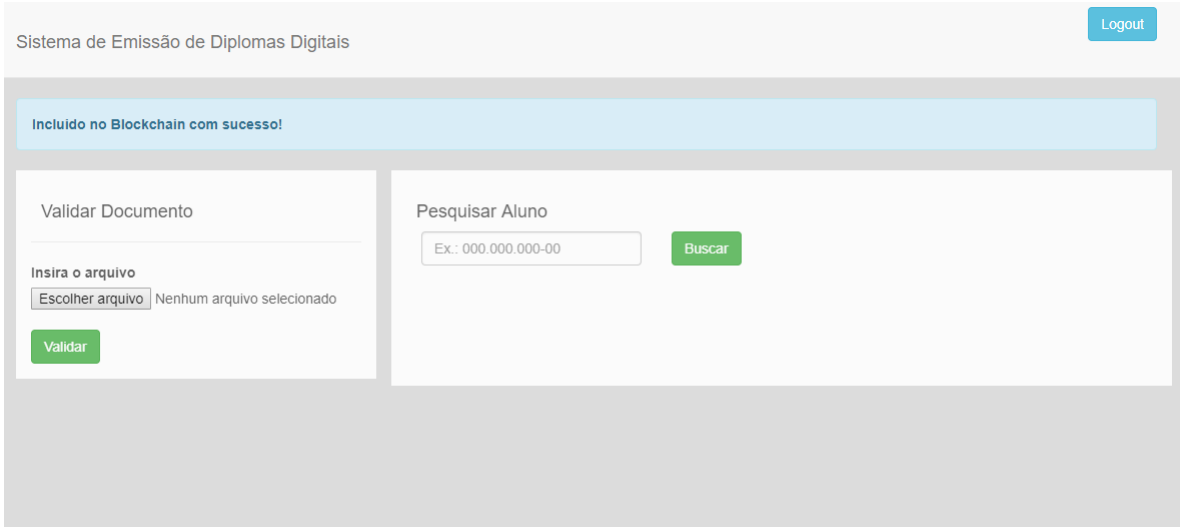
Código 3.4 – Código de inserção da hash do diploma na Blockchain local

```
1  module.exports.gravar = function(application, req, res){
2
3    if(req.session.autorizado !== true){
4      res.render("index", {validacao: {}});
5      return;
6    }
7
8    var connection = application.config.dbConnection;
9    var DiplomaDAO = new application.app.models.DiplomaDAO(connection);
10   var url_query = req.query;
11
12   fs.readFile('docs/'+url_query.nome.toUpperCase()+'_'+url_query.cpf+'_'
       +url_query.curso.toUpperCase()+'.pdf','utf-8', function(err,
       dataresult) {
13      if(err){
14          res.redirect("home?msg=C");
15          return;
16      }else{
17          datares = md5(dataresult);
18
```

```
19            url_query.hash = datares;
20
21            DiplomaDAO.gravar(url_query, res);
22
23            axios.post('http://localhost:3001/mineBlock', {
24                data : dateres
25            }).then((res) => {
26                console.log('statusCode : ${res.status}');
27            }).catch((error) => {
28                console.log(error);
29            });
30            res.redirect("home?msg=B");
31        }
32    }
33 }
```

A Blockchain local é executada em uma aplicação à parte, como explicaremos na próxima sessão, dessa forma os dados do diploma que serão inseridos em um novo bloco são enviados para a aplicação do Blockchain via POST, como podemos visualizar nas linhas de 23 a 29 da imagem acima, caso a inserção aconteça com sucesso a aplicação redireciona para a tela mostrada na Figura 12.

Figura 12 – Tela de confirmação ao inserir um novo valor na Blockchain



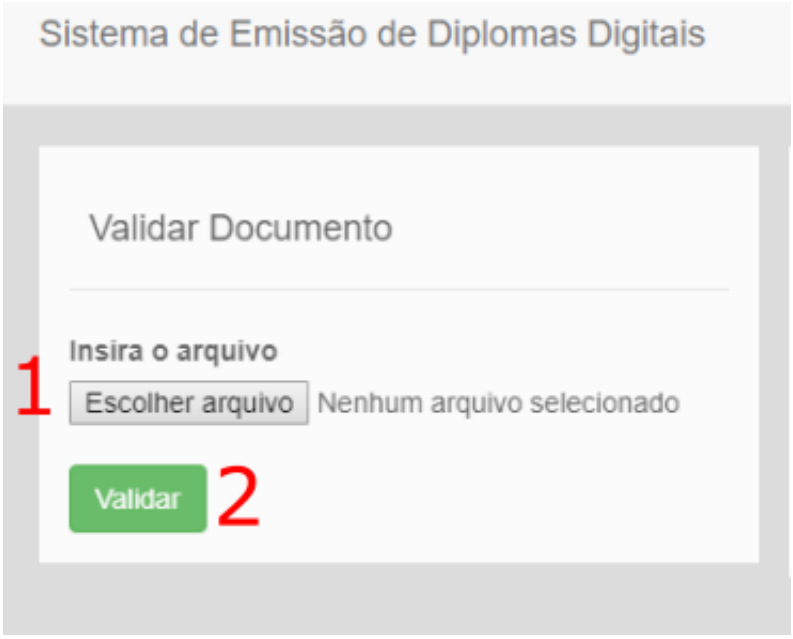
Fonte: O autor

3.2.3 Validação de Diploma

Outra funcionalidade de fundamental importância apresentada pelo sistema é a validação dos diplomas emitidos. Uma vez que o documento é gerado se faz necessário comprovar a sua autenticidade. Para isso utilizamos um procedimento que consiste em realizar o *upload* do arquivo no sistema, na área apropriada mostrada na Figura 13 e indicada pelo número 1, ao clicar no botão "Validar", indicado na figura com o número 2,

o sistema calcula o hash do arquivo inserido e verifica se este está armazenada na base de dados, em caso positivo, significa que ele também foi registrado na Blockchain e, dessa forma o documento é considerado autêntico.

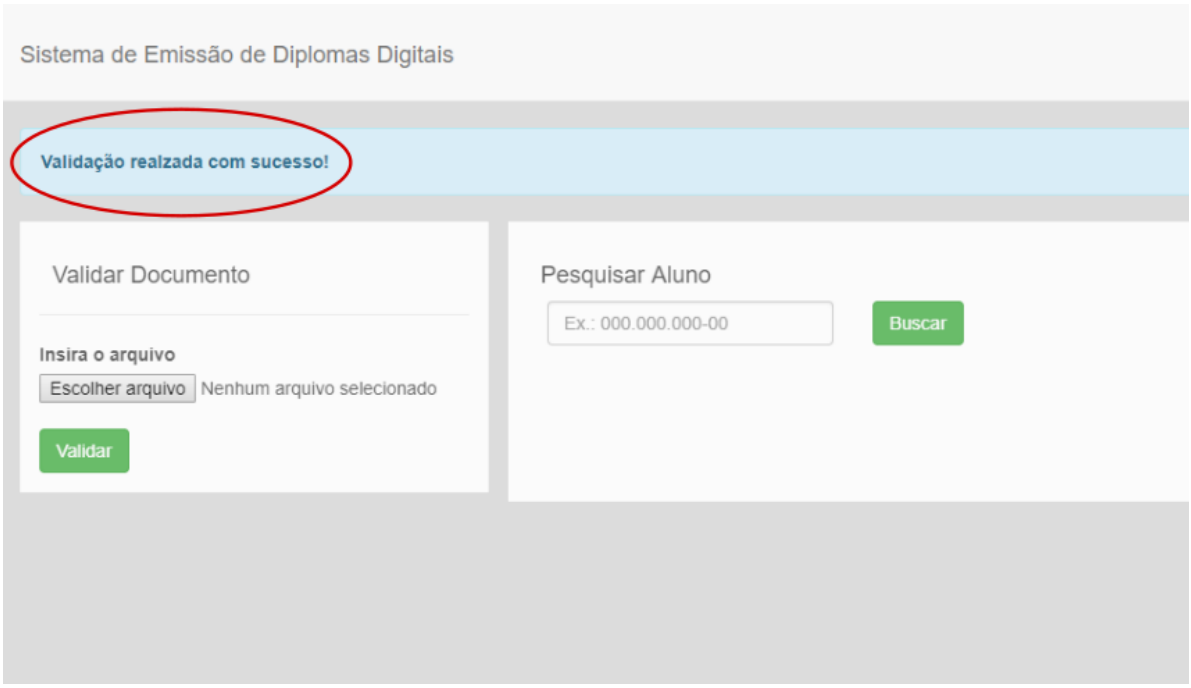
Figura 13 – Interface para validação de um documento



Fonte: O autor

Após a busca na base de dados, caso o registro do diploma seja localizado, é exibida uma mensagem de sucesso na tela inicial da aplicação informando ao usuário que a validação foi realizada com sucesso, como podemos visualizar na Figura 14.

Figura 14 – Validação de um diploma



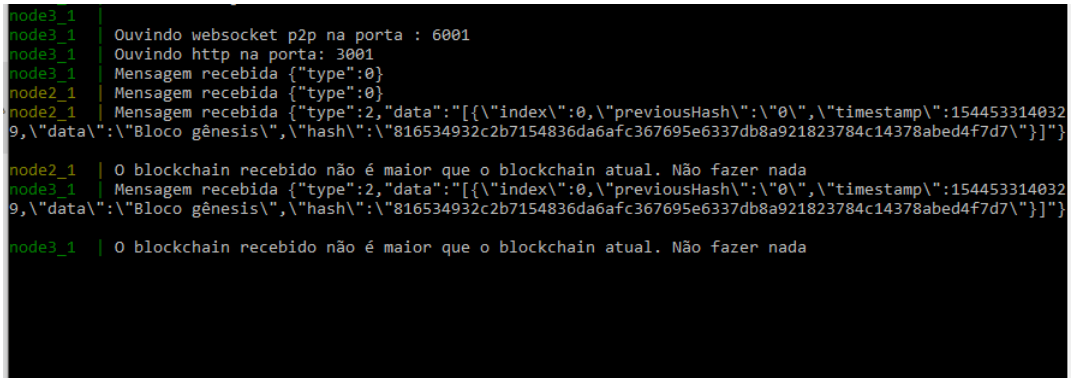
Fonte: O autor

3.3 Rede Blockchain local

Para a realização deste trabalho tomamos como base a aplicação desenvolvida por Mauro (2017), que implementa uma rede Blockchain de forma simples e didática em pouco mais de 200 linhas de código, utilizando Node.js. Realizamos alterações na referida aplicação e a integramos a este projeto, de forma a ser possível registrar os diplomas emitidos.

Ao ser executada, a rede Blockchain é criada contendo apenas o bloco gênesis e para simular a natureza distribuída da rede são criados três nós fazendo uso do Docker, cada nó recebe uma cópia exata da Blockchain e a partir de então começam a monitorar se os novos blocos adicionados são válidos e se podem ser acrescidos a rede. Na Figura 15, vemos o momento em que os nós 2 e 3 recebem o bloco gênesis que havia sido gerado no bloco 1.

Figura 15 – Os nós do blockchain contendo inicialmente apenas o bloco gênesis



Fonte: O autor

Para uma melhor visualização dos dados da Blockchain adicionamos um botão à tela inicial (indicado com 4 na Figura 8) que permite ao usuário visualizar as informações que já se encontram armazenados na rede, ao clicar neste botão, será exibida uma estrutura de blocos contendo as principais informações de cada bloco, como seu hash, o timestamp, o hash do bloco anterior e o valor armazenado por ele.

Mostramos na Figura 16, a representação visual do bloco gênesis, como se trata do primeiro da cadeia não existe nenhum bloco anterior a ele e o seu PreviousHash é zero, podemos visualizar também a data exata em que ele foi gerado, o hash que o identifica e o valor armazenado nele, que se trata apenas da *String* "Bloco gênesis".

Figura 16 – Blockchain local contendo apenas o bloco gênesis

Fonte: O Autor

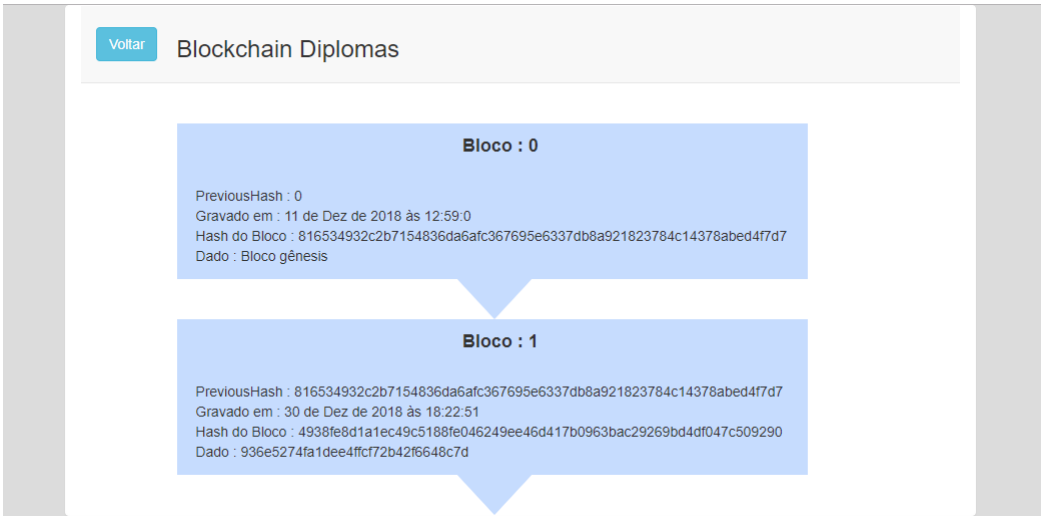
Na Figura 17, exibimos o momento em que o diploma da Figura 11 foi registrado na Blockchain. Podemos ver que todos os três nós da rede recebem os dados referentes ao novo bloco adicionado e que este contém exatamente o mesmo valor no atributo *data* que é o valor do hash do diploma, destacado na figura por linhas azuis.

Figura 17 – Os nós do Blockchain recebendo um novo nó

Fonte: O Autor

Por fim, mostramos na Figura 18, a representação gráfica da Blockchain após a inclusão do novo bloco.

Figura 18 – Imagem da Blockchain gerada pela aplicação após a geração de um documento



Fonte: O Autor

Como é possível ver, o bloco 1 foi criado e adicionado à cadeia, ele contém em seu atributo PreviouHash o valor do hash do bloco anterior, ou seja do bloco zero, nele podemos ver também a data e hora em que foi gerado, a hash que o identifica na cadeia de blocos e no atributo 'Dado' vemos a hash do diploma que foi gerado.

4 Considerações Finais

Neste capítulo, apresentamos as considerações finais acerca deste trabalho. Na sessão 4.1, discorreremos sobre os resultados obtidos e as contribuições que esta pesquisa poderá trazer para a sociedade. Na sessão 4.2, apresentaremos algumas possibilidades de trabalhos futuros que poderão ser desenvolvidos com base neste.

4.1 Conclusões

Neste trabalho, desenvolvemos uma proposta de aplicação que realiza o registro de diplomas digitais em uma rede Blockchain local e assim confere uma maior confiabilidade ao processo de validação destes documentos, uma vez que gravado em um Blockchain, um dado não pode mais ser alterado. A aplicação assegura também a integridade e disponibilidade dos dados que poderão ser consultados sempre que necessário.

Antes do desenvolvimento da aplicação pesquisamos sobre como se dá o processo de emissão de um diploma atualmente, como é feito o seu registro e quais leis regulamentam este processo. Buscamos ainda entender como é feita a verificação de autenticidade de um documento expedido por uma universidade, constatamos que o seu registro e validação é feito apenas de maneira manual, em livros de registros, o que pode acarretar em falsificações, ou mesmo perda ou danos dos livros arquivados.

Na revisão bibliográfica buscamos dar ênfase em estudar os princípios que regem a criação de estruturas de dados baseados em Blockchain, como é a estrutura de um bloco e como se dá o funcionamento da rede. Pudemos constatar que as redes Blockchain apresentam um alto nível de segurança e confiabilidade, e podem ser utilizadas para uma grande variedade de aplicações.

Por fim, especificamos os requisitos, funcionais e não-funcionais necessários à aplicação, e modelamos um sistema para emissão e validação de diplomas digitais utilizando os princípios de segurança da Blockchain.

4.2 Trabalhos futuros

Blockchain é uma tecnologia consideravelmente nova e por isso ainda existem inúmeras possibilidades a serem exploradas. Com base na abordagem proposta neste trabalho, sugerimos alguns trabalhos futuros que podem ser desenvolvidos para complemento deste e também para utilização em outras aplicações.

- **Criação e registro em Blockchain públicas:** Com o objetivo de conferir ainda mais segurança e confiabilidade ao sistema de emissão de diplomas, é desejável que o registro destes também seja realizado em uma Blockchain pública, a exemplo da rede Ethereum ou Decred. Assim, no momento da validação, o sistema verificará se o documento se encontra armazenado na base de dados local, na rede Blockchain local e também na rede pública, para só assim afirmar que este é autêntico.

- **Validar testes de integridade da Blockchain local vs remota:** Para assegurar a confiabilidade da aplicação se faz necessário a realização de testes da Blockchain local, avaliando a sua disponibilidade, integridade, tolerância a ataques, entre outras coisas. Uma vez que a aplicação for integrada a uma Blockchain pública novos testes deverão ser realizados para garantir a segurança e a integridade.

- **Criação de uma API para servir de suporte a futuras aplicações:** Para permitir que novas aplicações sejam criadas e até mesmo integradas à rede Blockchain local, é desejável a criação de uma API, que servirá de suporte para o desenvolvimento e facilitará a comunicação entre as aplicações, para isso, poderá ser feito uso da Loopback API, que é uma estrutura Node.js de código aberto altamente extensível que permite criar APIs REST dinâmicas, com pouca ou nenhuma codificação (IBM, 2018).

Referências

BALTE, A.; KASHID, A.; PATIL, B. Security Issues in Internet of Things (IoT): A Survey. *International Journal of Advanced Research in Computer Science and Software Engineering*, v. 5, n. 4, p. 450–455, 2015. ISSN 0953-4075. Citado na página 33.

BRAGA, A.; MARINO, F.; SANTOS, R. Segurança de Aplicações Blockchain Além das Criptomoedas. *Livro de minicursos do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'17)*, p. 99–148, 2017. Disponível em: <https://sbseg2017.redes.unb.br/wp-content/uploads/2017/04/20171107-SBSeg2017-Livro_de_Minicursos.pdf>. Citado 2 vezes nas páginas 36 e 37.

BRASIL. Decreto lei nº 2.848, de 7 de dezembro de 1940. Brasília, DF, dez 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 04.11.2018. Citado na página 24.

BRASIL. Lei nº 9.394, de 20 de dezembro de 1996. Brasília, DF, dez 1996. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/leis/L9394.htm>. Acesso em: 03.11.2018. Citado 2 vezes nas páginas 23 e 38.

BRASIL. Nota tecnica nº 391, de 24 de junho de 2013. Brasília, DF, jun 2013. Disponível em: <http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=13415-nota-tecnica-391-2013-expedicao-diplomas-registro-pdf&category_slug=junho-2013-pdf&Itemid=30192>. Acesso em: 25.11.2018. Citado na página 38.

BRASIL. Decreto nº 9.235, de 15 de dezembro de 2017. Brasília, DF, dez 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9235.htm#art107>. Acesso em: 25.11.2018. Citado na página 38.

BRASIL. Portaria nº 330, de 5 de abril de 2018. Diário Oficial da União, Brasília, DF, abr 2018. Disponível em: <https://www.capes.gov.br/images/stories/download/legislacao/06042018-Portaria-MEC-n-327-de-5-de-abril-de-2018.pdf>. Acesso em: 04.11.2018. Citado 2 vezes nas páginas 24 e 40.

DIEGO, M.; PAPAPANAGIOTOU, I.; YANG, B. Internet of things: Survey on security. *Information Security Journal*, v. 27, n. 3, p. 162–182, 2018. ISSN 19393547. Citado na página 33.

FERREIRA, E. et al. Uso de blockchain para privacidade e segurança em internet das coisas. p. 51, 11 2017. Disponível em: <https://sbseg2017.redes.unb.br/wp-content/uploads/2017/04/20171107-SBSeg2017-Livro_de_Minicursos.pdf>. Citado 6 vezes nas páginas 24, 29, 30, 31, 33 e 36.

GIL, A. C. *Métodos e Técnicas de Pesquisa Social*. 6ª. ed. São Paulo: Atlas, 2008. 8 p. ISBN 978-85-224-5142-5. Citado na página 25.

GULO, C. J. SeguranÇa da informaÇÃo. jan 2012. Disponível em: <https://www.researchgate.net/publication/265785308_SEGURANCA_DA_INFORMACAO>. Acesso em: 22.11.2018. Citado na página 35.

IBM. Loopback documentation. dez 2018. Disponível em: <https://loopback.io/doc/>. Acesso em: 06.01.2018. Citado na página 58.

ITI. Icp-brasil. Brasília, DF, jul 2017. Disponível em: <https://www.iti.gov.br/icp-brasil>. Acesso em: 25.11.2018. Citado na página 41.

ITI. Diploma digital em instituições de ensino superior será assinado com certificado icp-brasil. Brasília, DF, abr 2018. Disponível em: <https://www.iti.gov.br/noticias/indice-de-noticias/2307-diploma-digital-em-instituicoes-de-ensino-superior-sera-assinado-com-certificado-icp-brasil>. Acesso em: 25.11.2018. Citado na página 41.

MAURO, J. Uma blockchain em 200 linhas de código. out 2017. Disponível em: <https://medium.com/@johnsonmauro/uma-blockchain-em-200-linhas-de-c%C3%B3digo-96823f72637a>. Acesso em: 30.10.2018. Citado na página 53.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9. doi:10.1007/s10838-008-9062-0stem. *Journal for General Philosophy of Science*, v. 39, n. 1, p. 53–67, 2008. ISSN 09254560. Citado 2 vezes nas páginas 23 e 30.

ORIGINALMY. Registro de autenticidade. 2017. Disponível em: <https://originalmy.readthedocs.io/pt_BR/latest/00-apresentacao.html>. Acesso em: 22.11.2018. Citado 2 vezes nas páginas 34 e 35.

PILKINGTON, M. Blockchain technology: principles and applications. *Research Handbook on Digital Transformations*, p. 225–253, 09 2016. ISSN 1553-877X. Disponível em: <http://www.elgaronline.com/view/9781784717759.00019.xml>. Acesso em: 06.11.2018. Citado na página 24.

PRESSMAN, R. S. *Engenharia de software: uma abordagem profissional*. 6th. ed. Porto Alegre: Bookman, 2009. Citado na página 43.

PROOF. Entenda blockchain em menos de 15 minutos. 2017. Disponível em: <https://www.proof.com.br/blog/blockchain/>. Acesso em: 20.11.2018. Citado na página 29.

SOMMERVILLE, I. *Engenharia de software*. 8th. ed. São Paulo: Pearson, 2007. Citado na página 44.

STALLINGS, W. *Criptografia e Segurança de Redes, princípios e práticas*. 6ª. ed. São Paulo: Pearson, 2015. 7 p. ISBN 978-85-430-1450-0. Citado 2 vezes nas páginas 25 e 35.

SZABO, N. Smart contracts. 1994. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>. Acesso em: 23.11.2018. Citado na página 34.

TANENBAUM, A. S. *Sistemas Distribuídos, princípios e paradigmas*. 2ª. ed. São Paulo: Pearson, 2007. 1 p. ISBN 978-85-7605-142-8. Citado na página 23.

TECHNOLOGIES, B. Smart contracts explained: The ultimate guide to understanding blockchain smart contracts. 2018. Disponível em: <http://www.blockchaintechnologies.com/blockchain-smart-contracts>. Acesso em: 22.11.2018. Citado na página 33.

TEIXEIRA, L. F.; TAVARES, J. F. C. Blockchain: Dos conceitos às possíveis aplicações. p. 4–10, mar 2018. Disponível em: <https://www.researchgate.net/publication/327161498_Blockchain_Dos_Conceitos_as_Possiveis_Aplicacoes>. Acesso em: 22.11.2018. Citado 2 vezes nas páginas 32 e 34.

Anexos

ANEXO A – Diploma Digital (Portaria MEC)

Art. 9º Além das situações previstas em lei, a acumulação de bolsas pelos beneficiários deve ser considerada situação excepcional, somente admissível quando imprescindível para o atingimento das metas e objetivos do programa ou ação governamental, sem prejuízo dos demais.

Art. 10. A gestão das bolsas será realizada por meio de plataforma que permita o compartilhamento de dados entre o MEC e entidades vinculadas, para a realização de pesquisas, cruzamento de informações, produção de indicadores e avaliações necessárias ao aperfeiçoamento da gestão de bolsas.

Parágrafo único. O compartilhamento de dados de que trata o caput se dará por meio de disponibilização de base de dados das entidades vinculadas para acesso pelo MEC com frequência mensal.

CAPÍTULO IV

DAS COMPETÊNCIAS

Art. 11. Os agentes públicos, em todos os níveis e unidades, no âmbito de suas respectivas competências, são responsáveis pela boa gestão das bolsas concedidas, assim como pela estrita observância ao disposto nos art. 4º a 6º desta Política.

Art. 12. Compete aos dirigentes do MEC e entidades vinculadas assegurar que a formulação dos programas e política pública que prevejam a concessão de bolsas observe as disposições desta Política.

Art. 13. Compete aos bolsistas, o cumprimento dos compromissos específicos por eles formalmente assumidos no âmbito dos programas e política pública.

Art. 14. Compete à Secretaria-Executiva do MEC, com apoio das Unidades Administrativas e entidades vinculadas, supervisionar a implementação da política de gestão de bolsas no âmbito deste Ministério.

Parágrafo único. Sem prejuízo de outras solicitações que vierem a ser expedidas pela Secretaria-Executiva, o apoio referido no caput consiste:

I - na elaboração de relatórios gerenciais, com indicação dos valores pagos por programa ou política pública, situações de acumulação detectadas e outras informações julgadas necessárias à função supervisora; e

II - no exame das propostas de programas e política pública que envolvam a concessão de bolsas, quanto ao cumprimento aos requisitos dispostos nesta Portaria.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 15. Os casos omissos e as dúvidas surgidas na aplicação desta Política serão dirimidas pela Secretaria-Executiva.

PORTARIA Nº 328, DE 5 DE ABRIL DE 2018

Dispõe sobre a suspensão do protocolo de pedidos de aumento de vagas e de novos editais de chamamento público para autorização de cursos de graduação em Medicina e institui o Grupo de Trabalho para análise e proposição acerca da reorientação da formação médica.

O MINISTRO DE ESTADO DA EDUCAÇÃO, no uso da atribuição que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, e considerando os objetivos estabelecidos na Lei nº 12.871, de 22 de outubro de 2013, resolve:

Art. 1º Fica suspensa por cinco anos a publicação de editais de chamamento público para autorização de novos cursos de graduação em Medicina, nos termos do art. 3º da Lei nº 12.871, de 22 de outubro de 2013, e o protocolo de pedidos de aumento de vagas em cursos de graduação em Medicina ofertados por instituições de educação superior vinculadas ao sistema federal de ensino, de que trata o art. 40 do Decreto nº 9.235, de 15 de dezembro de 2017.

Parágrafo único. A suspensão do protocolo de pedidos de aumento de vagas de que trata o caput não se aplica aos cursos de Medicina autorizados no âmbito dos editais de chamamento público em tramitação ou concluídos, segundo o rito estabelecido no art. 3º da Lei nº 12.871, de 2013, e aos cursos de Medicina pactuados no âmbito da política de expansão das universidades federais, cujos pedidos de aumento de vagas poderão ser solicitados uma única vez e analisados de acordo com regras e calendário específicos, a serem definidos pelo Ministério da Educação - MEC.

Art. 2º Em função do disposto no art. 1º, fica instituído Grupo de Trabalho - GT, no âmbito do MEC, para subsidiar a reorientação da formação médica em cursos de graduação em Medicina.

Art. 3º O GT ficará vinculado ao Gabinete da Secretaria de Regulação e Supervisão da Educação Superior - SERES e será composto por representantes de cada um dos seguintes órgãos e entidades:

I - Secretaria de Regulação e Supervisão da Educação Superior do Ministério da Educação - SERES-MEC;

II - Secretaria de Educação Superior do Ministério da Educação - SESu-MEC;

III - Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira - Inep;

IV - Empresa Brasileira de Serviços Hospitalares - Ebserh;

V - Conselho Nacional de Educação - CNE;

VI - Conselho Federal de Medicina - CFM;

VII - Associação Médica Brasileira - AMB; e

VIII - Associação Brasileira de Educação Médica - ABEM.

§ 1º Os representantes, titular e suplente, deverão ser indicados pelos dirigentes máximos dos respectivos órgãos e entes, no prazo de quinze dias, a contar da publicação desta Portaria.

§ 2º As atividades do GT serão iniciadas no prazo de trinta dias após a publicação desta Portaria.

§ 3º O GT reunir-se-á periodicamente, conforme cronograma a ser definido e divulgado pela SERES, que coordenará as atividades.

§ 4º A participação no GT não ensejará remuneração para os seus membros e os trabalhos nele desenvolvidos serão considerados prestação de relevante serviço público.

Art. 4º O GT deverá apresentar relatórios e estudos a fim de subsidiar a política de formação médica e as ações regulatórias do MEC para a autorização de novos cursos de Medicina, considerando aspectos de qualidade dos cursos de graduação em Medicina em funcionamento, de inserção regional quanto aos serviços de atendimento à saúde, de inclusão dos egressos e de condição de oferta.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

MENDONÇA FILHO

PORTARIA Nº 329, DE 5 DE ABRIL DE 2018

Dispõe sobre a autorização e o funcionamento de cursos de graduação em Medicina nos sistemas de ensino dos estados e do Distrito Federal.

O MINISTRO DE ESTADO DA EDUCAÇÃO, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso II, da Constituição, e tendo em vista o disposto no art. 6º da Lei nº 4.024, de 20 de dezembro de 1961, com redação dada pela Lei nº 9.131, de 24 de novembro de 1995; nos arts. 8º, § 1º, 9º, inciso VII, e 46, § 5º, da Lei nº 9.394, de 20 de dezembro de 1996; em conformidade com a Lei nº 12.871, de 22 de outubro de 2013; com o Decreto nº 9.005, de 14 de março de 2017; e com o art. 41, § 2º, do Decreto nº 9.235, de 15 de dezembro de 2017, resolve:

Art. 1º Os sistemas de ensino dos Estados e do Distrito Federal deverão adotar os critérios definidos na Lei nº 12.871, de 22 de outubro de 2013, nos termos definidos pelo art. 46, § 5º, da Lei nº 9.394, de 1996, para a autorização e o funcionamento de cursos de graduação em Medicina.

Parágrafo único. Os processos de autorização de cursos de graduação em Medicina nos estados e no Distrito Federal deverão ser precedidos de procedimento de chamamento público para seleção de municípios e de propostas das instituições públicas de ensino superior dos seus respectivos sistemas de ensino.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

MENDONÇA FILHO

PORTARIA Nº 330, DE 5 DE ABRIL DE 2018

Dispõe sobre a emissão de diplomas em formato digital nas instituições de ensino superior pertencentes ao sistema federal de ensino.

O MINISTRO DE ESTADO DA EDUCAÇÃO, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, em observância ao art. 6º da Lei nº 4.024, de 20 de dezembro de 1961, com redação dada pela Lei nº 9.131, de 24 de novembro de 1995, bem como o disposto nos arts. 9º e 16 da Lei nº 9.394, de 20 de dezembro de 1996, resolve:

Art. 1º Fica instituído o Diploma Digital no âmbito das instituições de ensino superior, públicas e privadas, pertencentes ao sistema federal de ensino.

§ 1º O Diploma Digital abrange o registro e o respectivo histórico escolar.

§ 2º A emissão do Diploma Digital fica restrita às instituições que dispõem da prerrogativa para emissão e registro de diploma conforme os arts. 48, § 1º; 53, inciso VI; e 54, § 2º, da Lei nº 9.394, de 20 de dezembro de 1996, e de acordo com o Decreto nº 9.235, de 15 de dezembro de 2017, e a Resolução CNE/CES nº 12, de 13 de dezembro de 2007.

Art. 2º A adoção do meio digital para expedição de diplomas e documentos acadêmicos deverá atender as diretrizes de certificação digital do padrão da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, disciplinado em lei, normatizado e fixado pelo Instituto Nacional de Tecnologia da Informação - ITI, para garantir autenticidade, integridade, confiabilidade, disponibilidade, rastreabilidade e validade jurídica e nacional dos documentos emitidos.

Art. 3º Os procedimentos gerais para emissão de documentos por meio digital e para a expedição e o registro de diplomas digitais serão regulamentados em ato específico do Ministério da Educação.

Art. 4º As instituições de ensino superior terão vinte e quatro meses para implementar o Diploma Digital após a data de publicação do regulamento previsto no art. 3º.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

MENDONÇA FILHO

PORTARIA Nº 331, DE 5 DE ABRIL DE 2018

Institui o Programa de Apoio à Implementação da Base Nacional Comum Curricular - ProBNCC e estabelece diretrizes, parâmetros e critérios para sua implementação.

O MINISTRO DE ESTADO DA EDUCAÇÃO, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso II, da Constituição, e considerando a necessidade de estabelecer ações conjuntas entre os entes federados que propiciem a melhoria da qualidade da educação, em conformidade com a Lei nº 9.394, de 20 de dezembro de 1996 - Lei de Diretrizes e Bases da Educação, com o Plano Nacional de Educação - PNE, instituído pela Lei nº 13.005, de 25 de junho 2014, em especial com vistas ao cumprimento de suas Metas 1, 3 e 7, e consoante a Base Nacional Comum Curricular - BNCC, homologada conforme os termos da Resolução CNE/CP nº 2, de 22 dezembro de 2017, resolve:

CAPÍTULO I

DO PROGRAMA

Art. 1º Fica instituído o Programa de Apoio à Implementação da Base Nacional Comum Curricular - ProBNCC, com vistas a apoiar a Unidade da Federação - UF, por intermédio das Secretarias Estaduais e Distrital de Educação - SEDEs e das Secretarias Municipais de Educação - SMEs, no processo de revisão ou elaboração e implementação de seus currículos alinhados à BNCC, em regime de colaboração entre estados, Distrito Federal e municípios.

Art. 2º O Programa utilizará como instrumentos de apoio:

I - assistência financeira às SEDEs, com vistas a assegurar a qualidade técnica, a construção em regime de colaboração entre estados, Distrito Federal e municípios e a disseminação dos currículos elaborados à luz da BNCC;

II - formação das equipes técnicas de currículo e gestão das SEDEs e SMEs; e

III - assistência técnica para as SEDEs, para a gestão do processo de implementação da BNCC junto às SMEs.

Art. 3º A participação no Programa dar-se-á mediante assinatura do Termo de Adesão, constante dos Anexos, pelo Secretário Estadual ou Distrital de Educação e pelo Presidente da Seccional da União Nacional dos Dirigentes Municipais de Educação - Undime do estado, e posterior encaminhamento do Termo à Secretaria de Educação Básica do Ministério da Educação - SEB-MEC.

Parágrafo único. Ao assinar o Termo de Adesão, as SEDEs e as Seccionais da Undime comprometem-se com o planejamento conjunto e com a utilização dos recursos provenientes do Programa, para viabilizar a implementação da BNCC, tanto nas redes estaduais quanto nas redes municipais.

CAPÍTULO II

DA ASSISTÊNCIA FINANCEIRA ÀS SEDEs

Art. 4º O Programa disponibilizará assistência financeira às SEDEs para viabilizar os seguintes serviços:

I - assessoria de especialistas em currículo, oriundos de instituições de pesquisa, universidades, consultorias independentes, entre outros;

II - logística de eventos e mobilizações dos sistemas e redes estaduais, distrital e municipais de ensino para a discussão e formação sobre a BNCC e o currículo, e contratação de palestrantes e facilitadores, entre outros; e

III - impressão de documentos preliminares e finalizados para a discussão e formação dos currículos.

Parágrafo único. A assistência financeira de que trata o caput será liberada nos moldes operacionais e regulamentares do Plano de Ações Articuladas - PAR, nos termos da Lei nº 12.695, de 25 de julho de 2012, e a Resolução nº 14, de 8 de junho de 2012, do Conselho Deliberativo do Fundo Nacional de Desenvolvimento da Educação - CD-FNDE, de acordo com os critérios de atendimento do Programa, e ratificados pela SEB-MEC.

Art. 5º Para receber a assistência financeira do Programa, os estados e o Distrito Federal deverão cumprir os seguintes requisitos no módulo PAR/SIMEC:

I - assinatura de termo de compromisso;

II - inserção de plano de trabalho, assinado conjuntamente com a Seccional da Undime no estado, contendo cronograma de atividades previstas alinhado ao cronograma geral divulgado pela SEB;

III - inserção de termos de referência construídos conjuntamente com a Seccional da Undime no estado; e

IV - inserção de publicação em Diário Oficial da UF, com membros da Comissão Estadual de Construção do(s) Currículo(s), tendo o Secretário Estadual ou Distrital de Educação e o Presidente da Seccional da Undime no estado em sua composição.

Parágrafo único. O recebimento da assistência financeira está condicionado à avaliação de mérito dos documentos referidos no caput, que será realizada pela SEB-MEC, e pela avaliação financeira, que será realizada pelo Fundo Nacional de Desenvolvimento da Educação - FNDE.

Art. 6º A assistência financeira será proporcional à quantidade de estabelecimentos estaduais e municipais públicos de educação infantil e escolas estaduais e municipais públicas de ensino fundamental em cada UF, segundo dados do último Censo Escolar disponível.