

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

ANDERSON MELO DE MORAIS

**BLOCKMOODLE: UMA SOLUÇÃO PARA INTEGRAÇÃO DE  
AMBIENTES VIRTUAIS DE APRENDIZAGEM A  
BLOCKCHAIN**

Recife  
2021

ANDERSON MELO DE MORAIS

**BLOCKMOODLE: UMA SOLUÇÃO PARA INTEGRAÇÃO  
DE AMBIENTES VIRTUAIS DE APRENDIZAGEM A  
BLOCKCHAIN**

Trabalho de Dissertação submetido à Universidade Federal Rural de Pernambuco, como requisito necessário para obtenção do grau de Mestre em Informática Aplicada sob a orientação do prof. dr. Fernando Antonio Aires Lins e coorientação do prof. dr Sérgio Francisco Tavares de Oliveira Mendonça.

Recife  
2021

Dados Internacionais de Catalogação na Publicação  
Universidade Federal Rural de Pernambuco  
Sistema Integrado de Bibliotecas  
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

---

- M827b      Morais, Anderson Melo de  
              BlockMoodle: uma solução para integração de ambientes virtuais de aprendizagem a Blockchain / Anderson Melo de  
              Morais. - 2021.  
              77 f. : il.
- Orientador: Fernando Antonio Aires Lins.  
              Coorientador: Sergio Francisco Tavares de Oliveira Mendonca.  
              Inclui referências.
- Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Pós-Graduação em Informática  
              Aplicada, Recife, 2021.
1. Blockchain. 2. Educação. 3. Segurança da informação. 4. Moodle. I. Lins, Fernando Antonio Aires, orient. II.  
              Mendonca, Sergio Francisco Tavares de Oliveira, coorient. III. Título

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

ANDERSON MELO DE MORAIS

Este Trabalho de Dissertação foi julgado adequado para a obtenção do título de Mestre em Informática Aplicada, sendo aprovado em sua forma final pela banca examinadora:

---

Orientador: Prof. Dr. Fernando Antonio  
Aires Lins  
Universidade Federal Rural de Pernambuco -  
UFRPE

---

Prof. Dr. Jorge da Silva Correia Neto  
Universidade Federal Rural de Pernambuco -  
UFRPE

---

Prof. Dr. Robson Wagner Albuquerque de  
Medeiros  
Universidade Federal Rural de Pernambuco -  
UFRPE

---

Prof. Dr. Obionor de Oliveira Nóbrega  
Universidade Federal Rural de Pernambuco -  
UFRPE

Recife, 25 de fevereiro de 2021





# Agradecimentos

Sou grato a Jesus e a sua Mãe Maria Santíssima, que me ajudaram a concluir este trabalho e chegar ao final do mestrado.

A minha mãe e aos meus familiares que sempre acreditaram em meu potencial e me incentivaram a ir mais longe.

Ao meu orientador o prof. Fernando Aires, sou muito grato por sua disponibilidade, incentivo e pelas valiosas lições que aprendi ao longo desses projeto, as levarei sempre comigo.

Ao meu coorientador o prof. Sérgio Mendonça, que tanto contribuiu para a realização deste trabalho.

A Maria Dayanne, que esteve ao meu lado durante este curso, acreditando em mim e me incentivando a seguir em frente.

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





*“Seja humilde para evitar o orgulho,  
mas voe alto para alcançar a sabedoria.”  
(Santo Agostinho)*



# Resumo

A educação apresenta-se como uma das áreas mais relevantes da sociedade, sendo ela responsável por promover o desenvolvimento pessoal dos indivíduos e consequentemente do meio em que eles estão inseridos. Na educação são geradas grandes quantidades de dados, por isso faz-se necessário a utilização de mecanismos seguros de gerenciamento de dados, para evitar a falsificação de documentos, notas e certificados. A modalidade de Ensino a Distância (EAD) tem se tornado cada vez mais popular; nela os conteúdos dos cursos são disponibilizados em ambientes virtuais de aprendizagem (AVA), sendo o Moodle um dos mais conhecidos e adotado por instituições de ensino de todo o mundo. O Moodle permite a criação e gestão de cursos e atividades e a comunicação entre alunos e professores. Neste contexto de EAD é possível fazer uso do Blockchain para garantir a segurança, imutabilidade e disponibilidade dos dados educacionais gerenciados pelo Moodle, porém, ainda não há solução disponível, de acordo com o estado da arte, para a integração desses dados a Blockchain. Este trabalho propõe a BlockMoodle, uma solução desenvolvida para integrar o ambiente Moodle a Blockchain Ethereum. Esta solução visa garantir confiabilidade, integridade e disponibilidade aos dados acadêmicos. Com o objetivo de avaliar a solução proposta, analisa-se o custo financeiro necessário ao uso da ferramenta, considerando valores reais da criptomoeda Ether. Também é realizada uma avaliação de desempenho para estimar seu comportamento em diferentes cenários de uso. Por fim, são apresentados trabalhos futuros associados à continuidade deste projeto.

**Palavras-chave:** Blockchain, Educação, Segurança da Informação, Moodle.



# Abstract

Education presents itself as one of the most relevant areas of society, being responsible for promoting the personal development of individuals and consequently the environment in which it is inserted. In education, large amounts of data are constantly generated, so it is necessary to use secure data management mechanisms to avoid falsifying documents, notes, and certificates. The Distance Learning modality (EAD) has become increasingly popular, in it the course contents are made available in virtual learning environments (VLE), with Moodle being one of the best known and adopted by educational institutions worldwide. Moodle allows the creation and management of courses and activities and communication between students and teachers. It is possible to make use of Blockchain to ensure the security, immutability, and availability of educational data managed by Moodle, however, there is still no solution available, according to the state of the art, for the integration of this data into Blockchain. This work proposes BlockMoodle, a solution developed to integrate the Moodle environment with Blockchain Ethereum. This solution aims to guarantee the reliability, integrity, and availability of academic data. To evaluate the proposed solution, the financial cost necessary to use the tool is analyzed, considering real values of the Ether cryptocurrency. A performance evaluation is also carried out to estimate its behavior in different usage scenarios. Finally, future works related to the continuity of this project are presented.

**Keywords:** Blockchain, Education, Information Security, Moodle.



# Lista de ilustrações

|                                                                                                          |    |
|----------------------------------------------------------------------------------------------------------|----|
| Figura 1 – Metodologia utilizada para a realização deste trabalho. . . . .                               | 29 |
| Figura 2 – Estrutura dos blocos da Blockchain. . . . .                                                   | 31 |
| Figura 3 – Esquema de funcionamento de um <i>Smart Contract</i> . . . . .                                | 34 |
| Figura 4 – Instância do Moodle utilizada para a realização deste trabalho. . . . .                       | 36 |
| Figura 5 – Visão geral do funcionamento da Unicert. . . . .                                              | 41 |
| Figura 6 – Visão geral da plataforma EduCTX. . . . .                                                     | 43 |
| Figura 7 – Fluxo de emissão de um certificado digital utilizando Blockchain Ethereum. . . . .            | 45 |
| Figura 8 – Visão geral da proposta descrita por Liu et al. (2018). . . . .                               | 46 |
| Figura 9 – Representação do funcionamento da aplicação. . . . .                                          | 47 |
| Figura 10 – Visão geral do funcionamento da BlockMoodle. . . . .                                         | 53 |
| Figura 11 – Visão geral da integração da aplicação com a Ethereum. . . . .                               | 54 |
| Figura 12 – Código fonte do <i>Smart Contract</i> utilizado pelo BlockMoodle. . . . .                    | 56 |
| Figura 13 – Tela de login da aplicação BlockMoodle. . . . .                                              | 57 |
| Figura 14 – Módulos contendo as funcionalidades disponíveis na aplicação. . . . .                        | 58 |
| Figura 15 – Interface de geração do histórico de notas do aluno. . . . .                                 | 58 |
| Figura 16 – Relatório de notas gerados pela BlockMoodle. . . . .                                         | 59 |
| Figura 17 – Realização do pagamento para inclusão do relatório na Blockchain. . . . .                    | 60 |
| Figura 18 – Tela de resumo dos relatórios de notas. . . . .                                              | 60 |
| Figura 19 – Mensagem de confirmação de autenticidade, exibida ao validar um documento. . . . .           | 61 |
| Figura 20 – Preço médio histórico anual do Gwei. . . . .                                                 | 64 |
| Figura 21 – Preço médio histórico anual do Ether em Dólar. . . . .                                       | 65 |
| Figura 22 – Vazão da aplicação BlockMoodle para diferentes quantidades de acessos simultâneos. . . . .   | 66 |
| Figura 23 – Tempo de resposta da BlockMoodle para diferentes quantidades de acessos simultâneos. . . . . | 67 |





# Lista de tabelas

|                                                     |    |
|-----------------------------------------------------|----|
| Tabela 1 – Comparativo de custos ano a ano. . . . . | 65 |
|-----------------------------------------------------|----|



# Lista de quadros

|                                                                                       |    |
|---------------------------------------------------------------------------------------|----|
| Quadro 1 – Comparativo dos trabalhos relacionados. . . . .                            | 48 |
| Quadro 2 – Requisitos Funcionais da BlockMoodle. . . . .                              | 51 |
| Quadro 3 – Requisitos não funcionais da BlockMoodle. . . . .                          | 52 |
| Quadro 4 – Tabelas do Moodle acessadas pelo BlockMoodle para coleta de dados. . . . . | 54 |



# Lista de abreviaturas e siglas

|        |                                                      |
|--------|------------------------------------------------------|
| AVA    | Ambiente Virtual de Aprendizagem                     |
| EAD    | Educação a distância                                 |
| PoW    | Proof-of-Work                                        |
| PoS    | Proof-of-Stack                                       |
| API    | Application Programming Interface                    |
| DApps  | Decentralized Applications                           |
| Moodle | Modular Object-Oriented Dynamic Learning Environment |



# Sumário

|          |                                                                                                        |           |
|----------|--------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Introdução</b>                                                                                      | <b>25</b> |
| 1.1      | Motivação                                                                                              | 26        |
| 1.2      | Objetivos                                                                                              | 27        |
| 1.2.1    | Objetivo geral                                                                                         | 27        |
| 1.2.2    | Objetivos específicos                                                                                  | 27        |
| 1.3      | Organização                                                                                            | 27        |
| <b>2</b> | <b>Metodologia</b>                                                                                     | <b>29</b> |
| <b>3</b> | <b>Fundamentação Teórica</b>                                                                           | <b>31</b> |
| 3.1      | Blockchain                                                                                             | 31        |
| 3.1.1    | Estrutura de um bloco                                                                                  | 32        |
| 3.1.2    | Mineração                                                                                              | 33        |
| 3.2      | <i>Smart Contracts</i>                                                                                 | 33        |
| 3.3      | Uso de Blockchain para atender aos princípios de segurança                                             | 35        |
| 3.4      | Moodle                                                                                                 | 36        |
| 3.5      | Considerações finais                                                                                   | 37        |
| <b>4</b> | <b>Trabalhos Relacionados</b>                                                                          | <b>39</b> |
| 4.1      | Uso de Blockchain para registro e validação de diplomas e certificados                                 | 39        |
| 4.2      | Uso de Blockchain para garantia de autenticidade, integridade e imutabilidade de documentos acadêmicos | 41        |
| 4.3      | Utilizando <i>Smart Contracts</i> em ambientes acadêmicos                                              | 44        |
| 4.4      | Registrando o conhecimento em Blockchain                                                               | 46        |
| 4.5      | Avaliação comparativa dos trabalhos                                                                    | 48        |
| 4.6      | Desafios de pesquisa em aberto                                                                         | 49        |
| 4.7      | Considerações finais                                                                                   | 50        |
| <b>5</b> | <b>BlockMoodle: Uma Solução para Integração de Ambientes Virtuais de Aprendizagem a Blockchain</b>     | <b>51</b> |
| 5.1      | Definição dos requisitos                                                                               | 51        |
| 5.1.1    | Requisitos funcionais                                                                                  | 51        |
| 5.1.2    | Requisitos não funcionais                                                                              | 52        |
| 5.2      | Visão Geral                                                                                            | 53        |
| 5.3      | Projeto e Implementação                                                                                | 55        |
| 5.3.1    | Ferramentas utilizadas                                                                                 | 55        |
| 5.3.2    | Implementação da solução BlockMoodle                                                                   | 55        |
| 5.4      | Considerações finais                                                                                   | 61        |
| <b>6</b> | <b>Avaliação</b>                                                                                       | <b>63</b> |
| 6.1      | Avaliação de custos financeiros                                                                        | 63        |

|                                  |                                                  |               |
|----------------------------------|--------------------------------------------------|---------------|
| 6.2                              | Avaliação de desempenho da BlockMoodle . . . . . | 65            |
| 6.3                              | Considerações finais . . . . .                   | 67            |
| <b>7</b>                         | <b>Conclusões e Trabalhos Futuros . . . . .</b>  | <b>69</b>     |
| 7.1                              | Conclusões . . . . .                             | 69            |
| 7.2                              | Contribuições . . . . .                          | 70            |
| 7.3                              | Trabalhos futuros . . . . .                      | 70            |
| <br><b>Referências . . . . .</b> |                                                  | <br><b>73</b> |



# 1 Introdução

Nos dias atuais, a tecnologia tem se tornado cada vez mais presente nos mais diversos âmbitos sociais. Diversas inovações têm surgido em áreas fundamentais da sociedade, como comunicação, saúde, entretenimento, e educação. Estas inovações têm permitido avanços relevantes, e a própria conjuntura mundial ocasionada pela pandemia COVID-19 requisitou o uso e pesquisa de tecnologias para sanar ou mitigar diversas questões envolvendo, por exemplo, o distanciamento social.

Mais especificamente na área de educação, um número crescente de pessoas tem buscado ter acesso ao ensino técnico e superior no Brasil, de forma presencial e também na modalidade de Ensino a Distância (EAD) (ARRUDA; ARRUDA, 2015). É possível afirmar também que, com a citada pandemia, a procura de cursos via educação a distância teve um considerável aumento (BROILO; NETO, 2021). Com isso, quantidades maiores de dados educacionais são gerados pelas instituições de ensino, como documentos acadêmicos, atividades, dentre outros. Com isso, surgem também novos desafios relacionados à segurança e privacidade desses dados.

Diante disto, cresce a importância da utilização de metodologias e recursos tecnológicos que assegurem a segurança e a integridade de dados educacionais. Neste contexto, um dos conceitos tecnológicos emergentes é o de Blockchain, que apresenta potencial para revolucionar a maneira como a informática é utilizada em contextos educacionais. Esta tecnologia pode ser utilizada com o objetivo de conferir mais segurança e confiabilidade aos processos educacionais (NGUYEN; DANG, 2018).

A tecnologia Blockchain foi lançada oficialmente ao mundo em 2008, e tinha como principal objetivo dar suporte à criação da criptomoeda Bitcoin (NAKAMOTO, 2008). Na época, diversos países enfrentavam uma severa crise financeira, que ocasionou instabilidades econômicas, falência de tradicionais bancos de investimento e enfraquecimento econômico mundial. Diante destes acontecimentos, a tecnologia Blockchain surgiu com o propósito de levar as transações financeiras para o meio digital e também tornar viável a sua execução de forma descentralizada, sem a necessidade de intermediários, como bancos ou instituições reguladoras.

A Blockchain é composta por múltiplas bases de dados distribuídas e criptografadas, que buscam garantir um alto nível de segurança dos dados descentralizando-os em diferentes locais (CHICARINO et al., 2017). Todas as interações ocorridas entre os usuários são agrupadas em estruturas de dados chamados blocos e estes, por sua vez, são distribuídos entre todos os computadores conectados à Blockchain. Um novo bloco, ao ser gerado, necessita ser validado para só então ser adicionado à cadeia. O registro dos blocos ocorre

de forma encadeada, onde cada um guarda uma referência para o seu anterior, o que impossibilita que novos dados sejam inseridos ou modificados sem que isso altere o encadeamento de todos os demais blocos da cadeia.

## 1.1 Motivação

Diante do alto nível de segurança observado no uso de Blockchain, surgiram diversas propostas de aplicação da tecnologia em diversas áreas, e dentre estas áreas está a educação (MORAIS; LINS, 2020b). Atualmente, é possível identificar problemas que são enfrentados por instituições de ensino, como por exemplo a necessidade do gerenciamento de toda a vida escolar dos alunos e a ocorrência de falsificação de diplomas e certificados. O aluno, ao necessitar mudar de curso ou de instituição, passa por inúmeros processos burocráticos para a realização de uma nova matrícula. Além disso, ao tentar ingressar no mercado de trabalho, o estudante necessita apresentar comprovações da formação recebida e das competências adquiridas, o que nem sempre se mostra uma tarefa simples (HARTHY; SHUHAIMI; ISMAILY, 2019).

Ainda na área de educação, com a popularização da Internet e o aumento do acesso a dispositivos como computadores e *Smartphones*, a modalidade de ensino a distância (EAD) tem se tornado cada vez mais popular e acessível a uma ampla parcela da população. No ensino EAD são utilizados ambientes virtuais de aprendizagem (AVA), para disponibilizar o conteúdo aos estudantes e permitir as interações entre alunos e professores. Um dos AVAs mais utilizados atualmente é o Moodle, que trata-se de um software livre e que oferece uma grande variedade de recursos, permitindo a criação e o gerenciamento de cursos, atividades, questionários, fóruns, dentre outros recursos (SABBATINI, 2007).

Em especial, com a pandemia originada pela COVID-19, existiu um aumento na procura e uso de ferramentas de ensino a distância (como AVAs) para atender a demanda de educação não presencial oriunda do cenário pandêmico. Com isto, uma quantidade ainda maior de dados tem sido gerada, e a questão de como tornar o gerenciamento desses dados mais seguro se tornou ainda mais relevante.

Neste contexto, alguns trabalhos propõem o uso de Blockchain na educação. Liu et al. (2018) sugere a criação de uma plataforma distribuída baseada em Blockchain para o registro de informações geradas pelos estudantes, como notas e histórico escolar. De forma semelhante, Zhong et al. (2019) apresentam uma plataforma para registrar os alunos e armazenar as informações de todas as suas atividades acadêmico/escolares, e um mecanismo de recompensa que premia o aluno pelas conquistas alcançadas. Han et al. (2018) propõem a criação de uma plataforma baseada em Ethereum que permite à instituição de ensino registrar os diplomas e certificados dos estudantes. Porém nenhum dos trabalhos encontrados atualmente na literatura são voltados à integração de AVAs

com Blockchain.

Neste cenário, torna-se importante a adoção de medidas de segurança que garantam a confiabilidade, integridade e disponibilidade dos dados acadêmicos registrados em um AVA. Assim, este trabalho busca propor uma solução para a integração de ambientes virtuais de aprendizagem (notadamente o Moodle) à Blockchain (no caso deste trabalho, Ethereum). Tal solução busca melhorar a segurança dos processos de emissão, validação e gerenciamento de documentos acadêmicos, como histórico de notas, atividades, dados pessoais de estudantes, dentre outros, mantendo todas essas informações registradas de forma permanente e criptografadas na Blockchain. Adicionalmente, o próprio conhecimento aprendido e gerado pelo aluno pode ser também armazenado e validado dentro da Blockchain, permitindo diversos trabalhos futuros interessantes.

## 1.2 Objetivos

A seguir são apresentados os principais objetivos que serão perseguidos ao longo deste trabalho.

### 1.2.1 Objetivo geral

Propor uma solução para integração de AVAs (Moodle) com Blockchain (Ethereum), buscando atender aos princípios de confidencialidade, integridade e disponibilidade.

### 1.2.2 Objetivos específicos

- Entender os princípios de segurança da tecnologia Blockchain e como ela pode ser aplicada em contextos educacionais;
- Especificar os elementos do Moodle que interagirão com a Blockchain; e projetar uma aplicação de gerenciamento de documentos acadêmicos integrada a uma Blockchain pública;
- Realizar avaliações de custo e desempenho da solução desenvolvida;

## 1.3 Organização

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

O Capítulo 2 apresenta a metodologia que foi utilizada para a realização deste trabalho. São descritos detalhes sobre o protocolo de pesquisa adotado para a execução da revisão de literatura.

O Capítulo 3 descreve os conceitos básicos fundamentais para o entendimento deste trabalho. A tecnologia Blockchain é apresentada e explica-se como se dá o seu funcionamento. O capítulo também descreve os *Smart Contracts* e a sua aplicabilidade, além de apresentar a plataforma Moodle e sua estrutura básica.

O Capítulo 4 apresenta os trabalhos relacionados ao uso de Blockchain em contextos educacionais existentes. São apresentados exemplos de projetos que utilizam Blockchain para diversas finalidades em contextos acadêmicos, como para o registro de diplomas e certificados, uso de Blockchain para garantia de autenticidade, integridade e imutabilidade de documentos acadêmicos, utilização de *Smart Contracts* em ambientes educacionais e registro de conhecimento em Blockchain.

O Capítulo 5 detalha a modelagem, projeto e implementação da BlockMoodle, que realiza a integração do AVA Moodle a Blockchain Ethereum. A ferramenta realiza o acesso a base de dados do Moodle e realiza a geração de relatórios em PDF, contendo dados sobre os cursos, disciplinas, alunos matriculados, atividades realizadas, histórico de notas, dentre outros. Os relatórios são registrados na rede Ethereum e podem ser validados sempre que necessário através do BlockMoodle.

No Capítulo 6 é realizada uma avaliação do custo financeiro necessário para a utilização da BlockMoodle. Também é elaborada uma avaliação de desempenho, simulando a aplicação de diferentes cargas de trabalho. O objetivo aqui é avaliar a solução proposta sobre óticas e requisitos não funcionais relevantes deste contexto, no caso custo e desempenho.

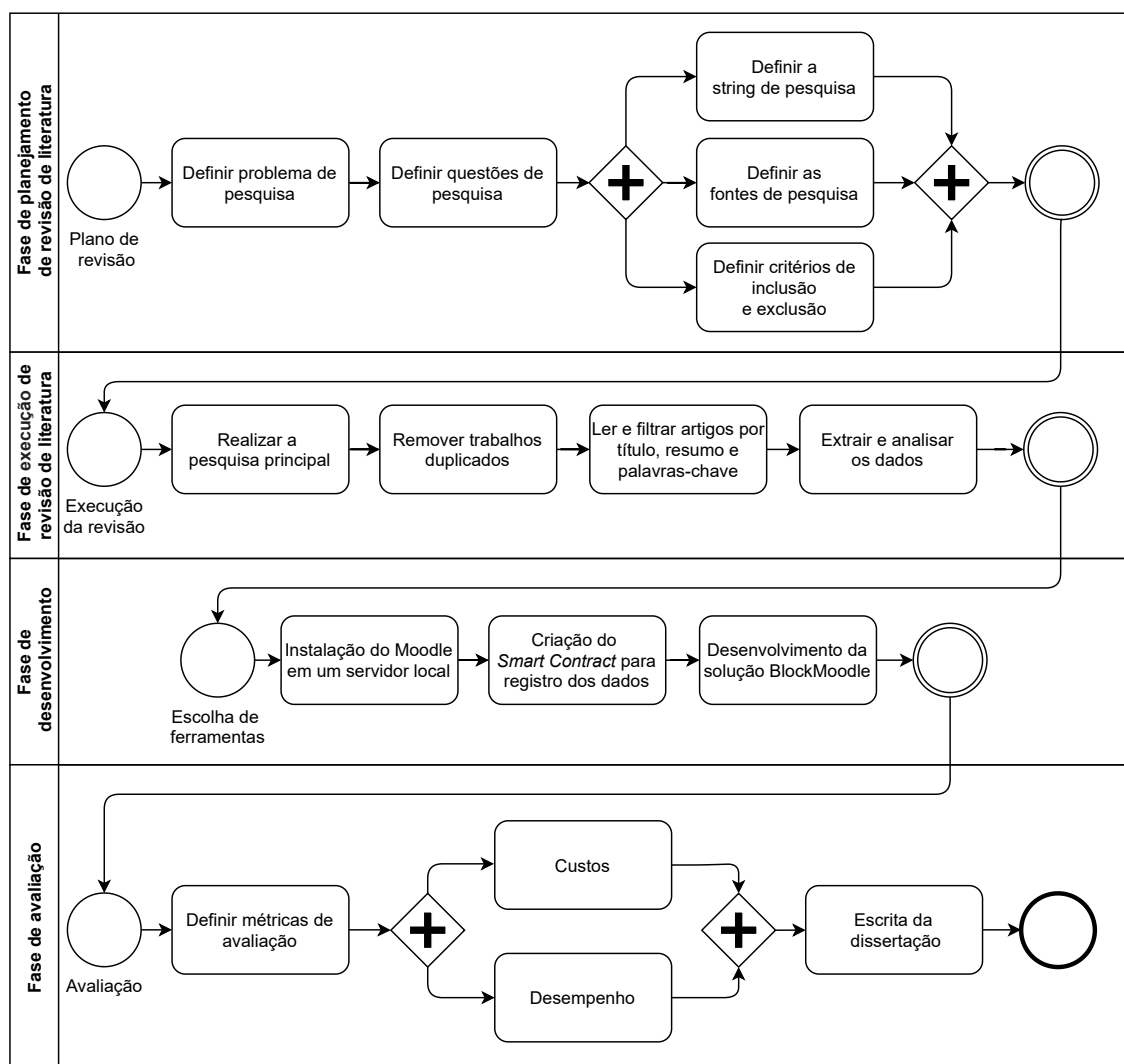
No Capítulo 7 são apresentadas as conclusões, principais contribuições e as possibilidades de trabalhos futuros que poderão ser realizados a partir desta dissertação.

## 2 Metodologia

A metodologia de pesquisa utilizada neste trabalho é proposta de acordo com a classificação de Provdanov e Freitas (2013). Quanto à natureza, este trabalho é categorizado como uma pesquisa aplicada, que tem como objetivo produzir conhecimento para uma aplicação prática, e assim apresentar solução para um problema específico.

Quanto ao método científico utilizado, este trabalho é classificado como hipotético-dedutivo. Segundo Gil (2008), este método parte de um dado problema, em seguida são formuladas conjecturas ou hipóteses que expressam as dificuldades geradas pelo problema. Essas hipóteses são utilizadas para fazer prognósticos, os quais serão comprovados ou não por meio de testes, experimentos ou observações mais detalhadas. A Figura 1 apresenta as etapas que compõem a metodologia utilizada no trabalho.

Figura 1 – Metodologia utilizada para a realização deste trabalho.



Fonte: O autor (2021).

Os objetivos de estudo deste trabalho são classificados como exploratórios, pois buscam proporcionar uma maior compreensão sobre um problema e formular hipóteses sobre ele. Esta pesquisa apresenta uma abordagem qualitativa, pois mantém o seu foco no entendimento, descrição, e generalização de um objeto de estudo específico.

Realizou-se uma pesquisa bibliográfica, através da busca de informações em materiais já publicados, como livros e publicações em periódicos científicos. Para a realização da pesquisa bibliográfica foram definidos os critérios de pesquisa, mediante a elaboração de um protocolo, conforme apresentado a seguir.

- **Questão de pesquisa:** como garantir confidencialidade, integridade e disponibilidade aos dados e documentos da EAD?
- **Bases científicas consultadas:** IEEE Xplore Digital Library; Springer Link; ACM Digital Library; Scielo; Google Scholar;
- **Palavras chave:** “Blockchain”, “education”, “data security”;
- **Critérios de inclusão:** artigos publicados após 2015 e que apresentam conteúdo relacionado a questão de pesquisa;
- **Critérios de exclusão:** trabalhos publicados antes de 2015 ou que apresentem conteúdo não relacionado ao tema de pesquisa;
- **Strings de busca:** “Blockchain AND Education”, “data security AND education”, “Blockchain AND Education AND data security”;

Após a definição do tema, iniciou-se a revisão bibliográfica, com o intuito de conhecer o atual estado da arte do uso de Blockchain em contextos educacionais. Foi possível identificar e classificar quatro principais aplicabilidades da tecnologia na educação, que foram: registro de diplomas; garantia de autenticidade de documentos acadêmicos; uso de *Smart Contracts* em contextos educacionais; e registro do conhecimento em Blockchain.

Em seguida foi realizado o desenvolvimento da ferramenta BlockMoodle, que realiza a integração do AVA Moodle à rede Blockchain Ethereum. A solução tem como base um *Smart Contract* que realiza o registro de diversas informações educacionais coletadas da base de dados do Moodle, como dados sobre cursos, atividades, notas, dentre outras.

Após a implementação foram efetuadas avaliações sobre a solução proposta. Realizou-se uma avaliação de custos financeiros da aplicação, com o objetivo de conhecer o valor a ser gasto com a geração de cada relatório, e uma avaliação de desempenho, para analisar o comportamento da BlockMoodle em diferentes cenários de uso. Por fim, foram realizadas ações para documentar, publicizar e proteger a pesquisa desenvolvida, como submissão de artigo em periódico (MORAIS; LINS, 2020b) e registro de software no Instituto Nacional de Propriedade Industrial (INPI) (MORAIS; LINS, 2020a).

## 3 Fundamentação Teórica

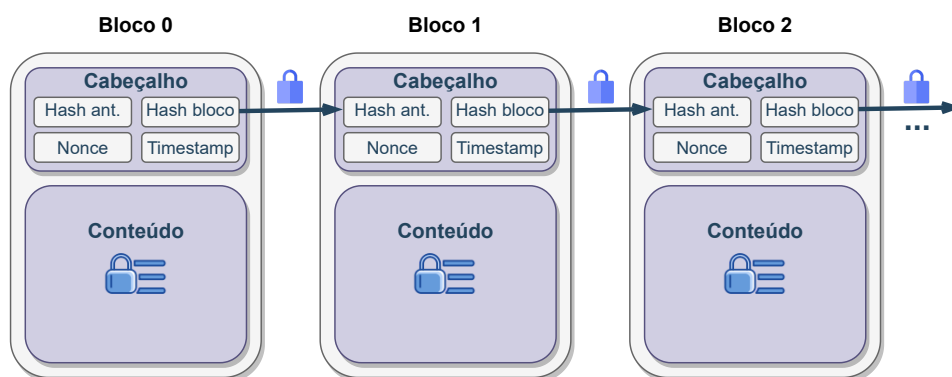
Neste capítulo são descritos conceitos fundamentais para a compreensão desse trabalho. A Seção 3.1 apresenta o conceito de Blockchain, como se dá o seu funcionamento e quais os princípios de segurança utilizados pela tecnologia. Na Seção 3.2 são descritos os *Smart Contracts* e sua aplicabilidade. A Seção 3.3 descreve como a tecnologia Blockchain pode ser utilizada para atender aos princípios fundamentais da segurança da informação. Na Seção 3.4 é apresentado o AVA Moodle, sua importância na EAD, e como é organizada a sua estrutura de dados. Por fim, a Seção 3.5 apresenta as considerações finais deste capítulo.

### 3.1 Blockchain

A tecnologia Blockchain tem como objetivo garantir a segurança através da descentralização dos dados. Seu funcionamento se dá através de bases de dados distribuídas, criptografadas e compartilhadas que armazenam informações sobre todas as transações que ocorrem entre os usuários da rede (CHICARINO et al., 2017). Todas estas informações são agrupadas em blocos e estes, por sua vez, são distribuídos entre os computadores conectados à rede, chamados nós. Se um novo bloco é inserido, todos os nós são atualizados para receber os novos dados e assim voltarem a conter o mesmo conteúdo.

Cada bloco possui um cabeçalho, que guarda informações relevantes de identificação do bloco como o *hash*<sup>1</sup> do bloco anterior, o *hash* de identificação do bloco e o *timestamp*, que registra o momento em que o bloco foi criado. Na Figura 2 é apresentada uma representação do encadeamento de blocos da Blockchain.

Figura 2 – Estrutura dos blocos da Blockchain.



Fonte: O autor (2021).

<sup>1</sup> O *hash* trata-se de um código numérico que garante que aquela transação é válida. Ao ser encontrado o bloco pode enfim ser adicionado à rede (NAKAMOTO, 2008).

No corpo do bloco está contido o conteúdo das transações. Os blocos são estruturas de dados que armazenam informações e são organizados em cadeia (WATTERS, 2016). Cada bloco guarda uma referência para o seu anterior; desta forma, é possível percorrer toda a cadeia até atingir o bloco inicial, também chamado bloco gênese. Tal bloco é gerado no momento da criação da rede e serve como o estado inicial do sistema, guardando informações sobre como a Blockchain deve operar durante todo o seu funcionamento.

Na Blockchain todas as transações entre os usuários ocorrem de forma criptografada, para isso, cada usuário possui uma chave pública e uma chave privada. A chave privada funciona como uma “senha” que permite assinar as transações ou enviar criptomoedas. É, portanto, a única informação necessária para acessar a Blockchain. Além disso, a chave privada protege a conta do usuário de ser acessada por outras pessoas. Já a chave pública funciona como o endereço do usuário na Blockchain, será utilizada para o envio de criptomoedas ou transações direcionadas a um usuário específico (SALOMAA, 2013).

Devido ao encadeamento dos blocos, não é possível que um deles seja modificado sem que isso seja percebido pelos demais, pois haverá a quebra do encadeamento. Para realizar uma alteração seria necessário gerar novamente todos os blocos posteriores da cadeia, o que em uma rede de grandes proporções se tornaria computacionalmente inviável.

### 3.1.1 Estrutura de um bloco

De acordo com Chicarino et al. (2017), um bloco é composto por duas partes principais, que são o cabeçalho e o corpo. No cabeçalho estão presentes diversos campos relativos ao protocolo em si, sendo os principais: o *hash* do bloco anterior; o *nonce*; a altura do bloco e o *hash* do cabeçalho, que têm a função de identificar o bloco e sua posição na Blockchain. O corpo armazena os dados das transações. A seguir são apresentados e descritos cada um desses conceitos (CHICARINO et al., 2017):

- **Transações:** consistem no conjunto de dados que são registrados nos blocos. Quando um novo nó é criado e validado, o conjunto de transações nele contido é enviado aos seus vizinhos, que por sua vez, reenviam aos demais, até que as informações sejam atualizadas em todos os nós da cadeia;
- **Hash do bloco anterior:** está presente no cabeçalho, e tem a finalidade de permitir o encadeamento dos blocos na cadeia, realizando a ligação do bloco atual ao seu anterior e assim sucessivamente. Dessa forma é possível percorrer toda a Blockchain, bloco a bloco, até atingir o bloco gênese. Por sua vez, o bloco gênese possui o campo *hash* do bloco anterior preenchido com zero, por não haver blocos anteriores a ele;
- **Hash do cabeçalho:** consiste no principal identificador do bloco na Blockchain. Após todas as informações terem sido validadas e incluídas no cabeçalho, o *hash*



do cabeçalho é gerado. É esta informação que é incluída no bloco posterior para garantir o encadeamento dos blocos;

- **Nonce:** consiste em um número usado como variável para alterar o resultado do *hash* gerado pelo cabeçalho. É utilizado para provar que um bloco foi minerado e atende aos requisitos determinados pela Blockchain;
- **Altura do bloco:** na Blockchain os blocos são incluídos de forma sequencial. A diferença entre a posição de um bloco e o bloco gênese da cadeia é denominada altura do bloco. Tal informação é importante no momento de localizar um determinado bloco dentro da cadeia;
- **Timestamp:** encontra-se no cabeçalho de cada bloco e consiste no registro do momento em que ele foi gerado e adicionado à cadeia. Este registro se dá através de um número que representa a data e hora da criação do bloco.

### 3.1.2 Mineração

É necessário realizar a validação de cada bloco, antes de inserir o mesmo na Blockchain. Isto é necessário para ser possível assegurar que ele está de acordo com os requisitos definidos pela rede. Essa validação, conhecida popularmente como mineração, consiste em um custoso procedimento computacional que busca encontrar um *hash* válido para o bloco.

Cada nó conectado à rede Blockchain armazena uma cópia do "livro-razão", que armazena o registro de todas as transações. Há alguns protocolos de mineração utilizados atualmente, sendo os mais conhecidos o de prova de trabalho (do inglês *Proof-of-Work* - PoW) e o de Prova de Participação (do inglês *Proof-of-Stake* - PoS), que se utilizam do poder de processamento das máquinas para solucionar cálculos matemáticos. Este processo é custoso computacionalmente, pois estes cálculos demandam um alto consumo de recursos, especialmente de processamento (CHICARINO et al., 2017).

O primeiro bloco da cadeia, chamado bloco gênese, é codificado pelo software e serve como o estado inicial do sistema. Ele contém informações sobre as regras ou instruções que os demais blocos deverão desempenhar. Em 2008 a primeira Blockchain foi lançada em código aberto ao mundo, no momento em que Satoshi Nakamoto realizou a mineração do bloco gênese da cadeia (NAKAMOTO, 2008).

## 3.2 Smart Contracts

Os *Smart Contracts* tratam-se de códigos computacionais capazes de facilitar, intermediar e executar o cumprimento de um acordo por meio da Blockchain, de forma

automática e segura. Os *Smart Contracts* apresentam um bom nível de segurança pois permitem que duas ou mais partes, mesmo distantes geograficamente e sem necessariamente se conhecerem, façam negócios entre si, não havendo a necessidade de uma entidade centralizada como intermediária.

O conceito de *Smart Contracts* surgiu na década de 1990, antes mesmo da existência das criptomoedas e das Blockchains, com o propósito de utilizar softwares para executar contratos (SZABO, 1994). Os contratos inteligentes recebem como entrada um conjunto de condições, que serão constantemente monitoradas e, ao serem satisfeitas, o contrato se auto executa. Todo o processo é automatizado e pode se dar de maneira totalmente virtual ou mista, como um complemento a contratos feitos no papel, tendo toda a segurança da transação garantida pela Blockchain.

A Figura 3 ilustra o funcionamento de um *Smart Contract*, onde no momento da codificação são definidas as condições do contrato, que poderão estar relacionadas a pagamentos, acordos de serviço, registro de dados pessoais, dentre outras coisas. Tais acordos podem ser realizados por indivíduos de quaisquer áreas, inclusive na educação. Em seguida o contrato é enviado à Blockchain.

Figura 3 – Esquema de funcionamento de um *Smart Contract*.



Fonte: O autor (2021).

Uma das maiores plataformas baseadas em Blockchain existentes atualmente é a Ethereum, que tem por finalidade permitir a programação de aplicações descentralizadas (DApps) e *Smart Contracts* (GENCER et al., 2018). A plataforma Ethereum busca ser um grande computador mundial com o seu poder de processamento distribuído em seus diversos nós. Neste contexto, o Ether é utilizado como moeda para a criação e gerenciamento dos contratos inteligentes e a compra de poder computacional.

De acordo com Teixeira e Tavares (2018), o processo de implementação, execução e funcionamento dos *Smart Contracts* é dividido em três etapas fundamentais, as quais são apresentadas a seguir:

- **Codificação:** inicialmente é realizada a codificação do contrato em alguma linguagem de programação. Na plataforma Ethereum a linguagem utilizada é a *Solidity*, que

permite definir as instruções que o contrato deve executar e que devem estar de acordo com o interesse das partes;

- **Envio à Blockchain:** após a codificação, o código é compilado e enviado a outros computadores por meio da Blockchain. Na Ethereum o envio de novas transações se dá mediante o pagamento de uma taxa, paga na criptomoeda Ether;
- **Execução.** Após o código fonte do *Smart Contract* ser recebido pela Blockchain, ele será executado em um de seus nós. Em seguida a rede fará a atualização dos registros para que os demais nós obtenham os resultados do processamento do contrato.

### 3.3 Uso de Blockchain para atender aos princípios de segurança

A informação tem se tornado cada vez mais valiosa em contextos financeiros, empresariais e educacionais. Logo é de fundamental importância que a informação seja armazenada, manipulada e divulgada de maneira segura (GULO, 2012). Para que uma aplicação seja considerada segura faz-se necessário cumprir alguns princípios, que segundo Stallings (2015) são integridade, disponibilidade e confidencialidade.

É possível fazer uso da tecnologia Blockchain para atender aos princípios de segurança mencionados anteriormente, conforme descrito a seguir:

- **Integridade:** este princípio assegura que as informações sejam modificadas somente de forma específica e autorizada. Com o registro em Blockchain é possível assegurar a integridade dos dados, devido ao fato de que as informações registradas nos blocos não podem ser modificadas, nem serem comprometidas por casualidades futuras, como panes elétricas ou falhas em uma bases de dados, pois se encontram armazenadas de forma distribuída;
- **Disponibilidade:** busca assegurar que um sistema esteja sempre pronto para desempenhar as suas funções. Este princípio é garantido pela Blockchain devido a sua descentralização, pois mesmo que alguns nós da rede fiquem temporariamente indisponíveis a Blockchain continuará operacional. As informações poderão ser acessadas a partir das diversas outras cópias existentes;
- **Confidencialidade:** busca assegurar que apenas indivíduos autorizados tenham acesso às informações e realizem operações sobre elas. Na cadeia de blocos os usuários são identificados através de um sistema de pseudo anonimato, através de endereços criptografados que são resumos de suas chaves públicas. Isso favorece o princípio da confidencialidade, pois somente indivíduos registrados podem ter acesso às informações disponíveis na aplicação.

## 3.4 Moodle

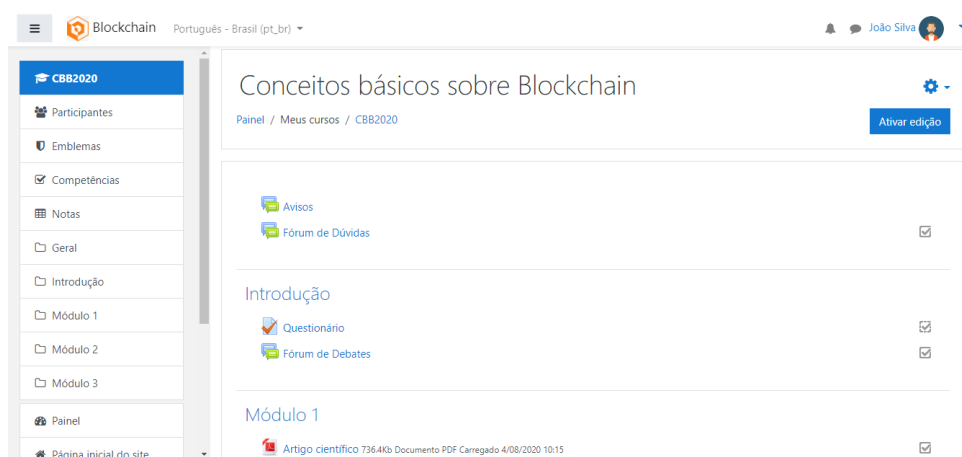
A palavra Moodle é uma sigla em inglês para *Modular Object-Oriented Dynamic Learning Environment*, que pode ser traduzida como “Ambiente de aprendizado modular orientado a objeto”. Trata-se de um software livre, cuja primeira versão foi lançada em 2002, e que se encontra em contínuo desenvolvimento e atualização por uma equipe de programadores do mundo todo (RÊGO; GARRIDO; MATOS, 2018).

De acordo com Sabbatini (2007) o Moodle é uma plataforma online e gratuita voltada para a educação a distância. Funciona como um sistema de gerenciamento de aprendizado, que oferece tanto a possibilidade de disponibilizar cursos e treinamentos de forma exclusivamente online como de ser usada para suporte a cursos presenciais.

A plataforma permite a disponibilização de diversos tipos de conteúdos aos estudantes, como páginas simples de texto, páginas em HTML, arquivos em diversos formatos (PDF, DOC, PPT, Flash, áudio, vídeo, etc.) ou links externos (URLs). Também podem ser ofertados livros eletrônicos, wikis (textos colaborativos) e glossários. O Moodle dispõe de diferentes ferramentas de interação, como chats para bate-papo, fórum de discussão e diários. Há ainda diversas ferramentas de avaliação, tais como avaliação do curso, questionários de avaliação, tarefas e exercícios.

Para o desenvolvimento deste trabalho, realizou-se a instalação do Moodle em uma máquina local, e criou-se um curso fictício intitulado "Conceitos básicos sobre Blockchain", conforme apresentado na Figura 4. Para os testes foram cadastrados 4 usuários, sendo um deles com o papel de professor e os demais como alunos. O curso possui 4 módulos, onde são disponibilizadas aos alunos atividades, como questionários, fórum de debates, glossário; além de materiais para estudo, como artigo científico e vídeo explicativo.

Figura 4 – Instância do Moodle utilizada para a realização deste trabalho.



Fonte: O autor (2021).

## 3.5 Considerações finais

Neste capítulo foram descritos os principais conceitos teóricos utilizados neste trabalho. Foi apresentada a tecnologia Blockchain, seus princípios de funcionamento e segurança. Descreveu-se a estrutura básica de um bloco e como ocorre o procedimento de mineração. Discorreu-se acerca dos *Smart Contracts*, o seu funcionamento de utilidade dentro do contexto educacional. Foi possível analisar como a tecnologia Blockchain pode ser utilizada para atender aos princípios básicos de segurança da informação. E por fim, foi apresentada e descrito o ambiente virtual de aprendizagem Moodle.



## 4 Trabalhos Relacionados

Este capítulo descreve as principais iniciativas de pesquisa relacionadas ao uso de Blockchain na educação. A Seção 4.1 descreve o uso de Blockchain para o registro e validação de diplomas. A Seção 4.2 trata do uso de Blockchain para a garantia de autenticidade de documentos acadêmicos. A Seção 4.3 apresenta as possibilidades de uso de *Smart Contracts* por instituições de ensino. A Seção 4.4 descreve o registro de conhecimento em Blockchain. Na Seção 4.5 é realizada uma avaliação comparativa dos trabalhos. A Seção 4.6 menciona os desafios em aberto na área. Por fim, na Seção 4.7 são apresentadas as considerações finais do capítulo.

### 4.1 Uso de Blockchain para registro e validação de diplomas e certificados

Ao considerar o uso de Blockchain em contextos educacionais, é possível notar que uma das principais discussões existentes atualmente recai sobre o registro de diplomas. Esta preocupação se deve ao fato do diploma ser um dos documentos mais importantes emitidos pelas instituições de ensino (GRECH; CAMILLERI, 2017). Ele serve como comprovação da formação recebida pelo estudante e lhe atribui a autorização necessária para exercer a sua profissão.

Nos últimos anos têm se tornado cada vez mais comum a busca por cursos na modalidade de Educação a Distância (EAD). Na oferta destes cursos são comumente utilizados recursos de Informática na Educação (PAULA et al., 2018). Nesta modalidade de ensino todo o processo se dá através de ambientes virtuais de aprendizagem (AVA), inclusive a disponibilização do diploma ou certificado do aluno ao final do curso. Porém, já houveram registros de diversos casos de falsificação de diplomas, o que pode comprometer a credibilidade das instituições de ensino, ou mesmo pôr a vida de pessoas em risco, ao inserir profissionais não qualificados no mercado. Diante disso, faz-se necessária a implementação de mecanismos de segurança robustos, que possam conferir uma maior confiabilidade ao processo de emissão e validação de diplomas (GALLARDO; BAZAN; VENOSA, 2019).

Segundo Harthy, Shuhaimi e Ismaily (2019), é possível realizar a utilização de Blockchain para assegurar uma maior segurança à emissão de diplomas, garantido que eles possam ser validados pelos possíveis interessados. Os autores apresentam quatro recomendações que, segundo eles, devem ser consideradas de forma geral ao utilizar Blockchain em instituições de ensino:

- **Definir as condições para execução da Blockchain.** É necessário que os nós sejam executados em máquinas que garantam um adequado poder de processamento à aplicação.
- **Definir qual método criptográfico será utilizado.** Deve-se conhecer o algoritmo que realizará o cálculo do hash dos blocos. O mais utilizado é o *SHA256*, que transforma um grande número de informações em uma sequência numérica hexadecimal de tamanho fixo.
- **Definir as regras de utilização de *Smart Contracts*.** Caso a aplicação faça uso de *Smart Contract*, é necessário definir suas regras de implementação e execução.
- **Rastreamento das transações.** É preciso garantir a rastreabilidade de todas as transações que ocorreram na rede e de todos os nós que foram minerados.

Embora apresente contribuições interessantes, o trabalho não apresenta implementações ilustrando a viabilidade de uso de Blockchain, o que reduz o entendimento sobre como esta solução poderia ser usada na prática.

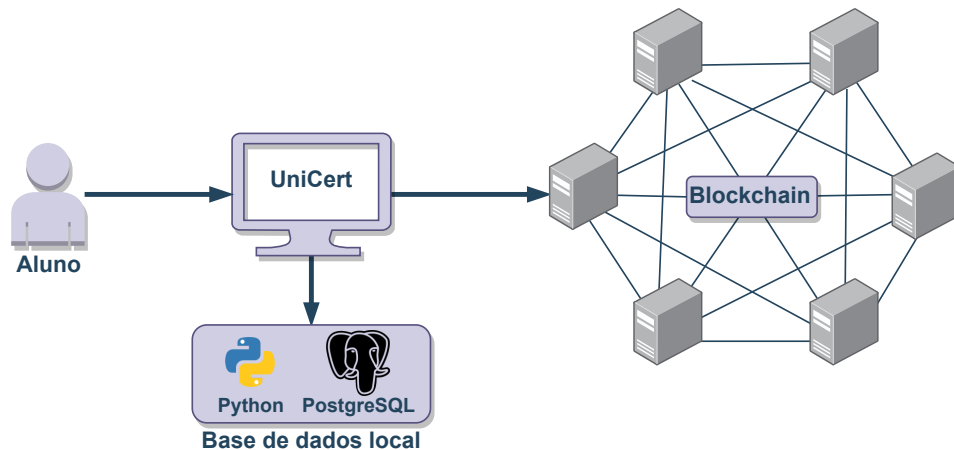
Para Kolvenbach, Ruland e Gräther (2018), é possível o desenvolvimento de uma plataforma baseada em Blockchain para controlar a emissão e validação de diplomas e certificados devido ao alto nível de segurança apresentado por esta tecnologia. O trabalho apresenta algumas ferramentas baseadas em Blockchain já existentes, desenvolvidas para este propósito: a Blockcerts (MIT, 2016), desenvolvida pelo MIT, e a TrueRec (BOESER, 2017), criada pelo grupo SAP.

Em seu trabalho, os recém citados autores descrevem a criação de uma nova plataforma, baseada em Ethereum, onde os diplomas podem ser registrados através de *Smart Contracts*. A instituição de ensino registra os dados do aluno no contrato, em seguida estes dados são validados por outras entidades de certificação. Após todo o processo, o diploma ou certificado poderá ser emitido e gravado na Blockchain, sendo possível a sua consulta por qualquer interessado, como empregadores ou outras instituições de ensino.

Uma proposta semelhante é apresentada por Huynh et al. (2018), onde os autores abordam a possibilidade de uso de Blockchain para a emissão e validação de certificados digitais visando garantir segurança e evitar falsificações. É proposta a criação do UniCert (Figura 5), uma aplicação que irá receber os dados dos certificados, realizar o seu registro em um banco de dados local PostgreSQL e enviar o *hash* do documento para os nós da rede Blockchain. Esta proposta apresenta um nível de segurança ainda maior em relação a outras propostas de uso de Blockchain, pois o registro é realizado em múltiplos níveis, na base de dados local e na Blockchain, o que torna ainda mais difícil a possibilidade de sucesso de ataques aos dados.



Figura 5 – Visão geral do funcionamento da Unicert.



Fonte: O autor (2021).

Em uma outra proposta, Kanan, Obaidat e Al-Lahham (2019) descrevem a modelagem e implementação do SmartCert, um sistema para emissão e validação de certificados, que realiza o registro dos documentos em Ethereum. A aplicação foi desenvolvida em uma Universidade utilizando dados reais dos estudantes. Após a definição dos requisitos, o SmartCert foi implementado contendo dois módulos principais: um deles permite à universidade realizar a inserção dos dados do aluno e de seus respectivos cursos e o outro permite ao estudante consultar os seus certificados.

Arenas e Fernandez (2018) apresentam o CredenceLedger, uma aplicação para verificação de credenciais acadêmicas. Ela realiza o acesso a uma rede Blockchain Ethereum, onde estarão armazenadas diversas informações sobre a trajetória acadêmica do aluno. Ao finalizar o curso, o estudante recebe uma cópia dos seus dados acadêmicos e o seu histórico em uma versão impressa e outra digital, autenticada pela plataforma. Futuramente, terceiros interessados poderão verificar a autenticidade destes documentos através da Blockchain.

## 4.2 Uso de Blockchain para garantia de autenticidade, integridade e imutabilidade de documentos acadêmicos

Existem diversos outros documentos acadêmicos, além dos mencionados na seção anterior, que precisam ser emitidos e armazenados de forma segura. Estes documentos são de grande importância na comprovação da formação recebida pelo aluno e de sua trajetória acadêmica. Dentre eles estão documentos como provas, históricos e currículo. É importante garantir que não haja, por exemplo, adulterações de notas por indivíduos mal intencionados.

Diante disto, Srivastava et al. (2019) sugerem a criação de uma plataforma para

registro de dados baseada em Blockchain que registra, através de *tokens*, todos os créditos adquiridos pelo estudante ao longo da sua trajetória acadêmica. Cada universidade integrante do sistema possui um nó na Blockchain e será responsável por gerar credenciais de identificação dos seus alunos mediante a verificação de autenticidade dos seus documentos pessoais.

Nesta proposta, cada aluno possui uma carteira digital, onde são registrados os *tokens* referentes a cada curso concluído por ele na instituição. Isto permite ao aluno comprovar, de maneira confiável, a formação recebida, e reduzirá os procedimentos burocráticos existentes caso o mesmo necessite mudar de instituição de ensino, pois os dados poderão ser consultados na própria Blockchain. O trabalho descreve a implementação da Blockchain utilizada no projeto e apresenta os principais algoritmos desenvolvidos, que têm como propósito cadastrar o aluno, cadastrar a instituição de ensino, realizar o consenso da rede, dentre outras funções.

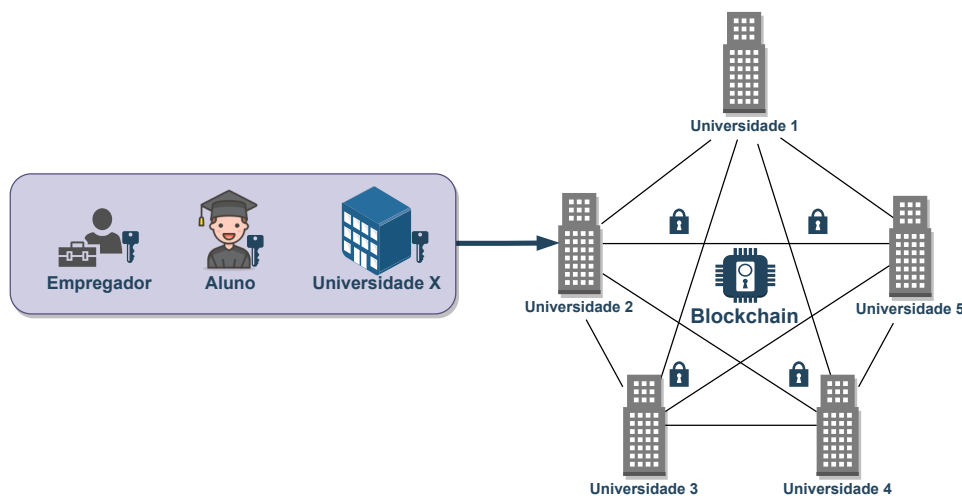
O trabalho proposto por Bore et al. (2017) apresenta o projeto, implementação e avaliação de um *Hub* de Informações Escolares integrado a uma Blockchain com o objetivo de descentralizar os dados e os manter seguros e acessíveis. Na proposta, todas as atividades e ocorrências escolares seriam registradas na forma de transações na Blockchain. Exemplos de transações incluem: cadastro de novos alunos, matrícula ou rematrícula em disciplinas, atualização da identidade do usuário, registro de frequência do aluno, etc.

Os autores apresentam um protótipo de implementação utilizando a rede *Hyperledger Fabric* (ANDROULAKI et al., 2018), onde é possível realizar o cadastro de alunos e professores, gerar identificadores (*hashs*) de documentos digitais e os inserir na rede. Por fim, os autores realizam um estudo de caso em uma escola do Quênia, utilizando dados reais de estudantes e professores.

Uma outra proposta inovadora é a plataforma EduCTX, apresentada por Holbl et al. (2018), que permite atribuir e gerenciar credenciais de indivíduos e instituições de ensino ou empresas. Uma visão geral desta plataforma é ilustrada na Figura 6. Na plataforma são registrados *tokens* que comprovam as capacidades do aluno, quais cursos ele já realizou, onde estudou, quais experiências profissionais ele possui, dentre outros dados. Todas estas informações podem ser consultadas por possíveis interessados, como empresas empregadoras ou instituições de ensino, o que pode evitar falsificações de documentos. De acordo com os autores, a plataforma foi desenvolvida para a plataforma Ethereum, fazendo uso de um *Smart Contracts* para realizar o registro das informações dos indivíduos e das transações ocorridas na rede.

Turkanović et al. (2018), em seu trabalho, também fazem referência à EduCTX. De acordo com os autores, trata-se de uma plataforma de crédito estudantil global baseada em Blockchain que visa evitar barreiras linguísticas e administrativas na hora de reconhecer a formação acadêmica de estudantes. Nela o estudante tem a vantagem de manter todo o seu

Figura 6 – Visão geral da plataforma EduCTX.



Fonte: O autor (2021).

histórico sempre acessível. De acordo com os autores, a Universidade Nacional de La Plata (PLATA, 2020) e a Faculdade CESYT (AMATI, 2015) da Argentina já utilizam outras soluções baseadas em Blockchain para registro de dados acadêmicos e emissão de diplomas. Na plataforma EduCTX, cada universidade é um nó na Blockchain, e armazena uma cópia da base de dados. Desta forma, as informações permanecem continuamente disponíveis para consulta por alunos, empregadores ou outras instituições de ensino interessadas mediante o uso de uma chave de acesso que funciona como identificador.

Em uma outra pesquisa, apresentada por Mikroyannidis et al. (2019), onde é proposta a utilização de Blockchain para auxiliar pesquisadores da área de ciência de dados. No trabalho é descrita a criação de uma base de registro de alunos, onde são armazenadas as suas habilidades, cursos e conquistas profissionais. A principal finalidade da plataforma é garantir a veracidade do histórico de formação do aluno e evitar falsificações. O sistema realiza recomendações de novos cursos de acordo com as áreas de interesse do estudante. A plataforma serve ainda como um sistema de recomendações de empregos, tomando como base as qualificações do aluno, recomendando as vagas que lhes são mais indicadas. De acordo com os autores a solução proposta, que faz uso da rede Ethereum, se encontra em fase de prototipação e até aquele momento não fazia uso de dados reais de estudantes.

Duan, Zhong e Liu (2018), por sua vez, propõem o uso de Blockchain para registrar toda a trajetória educacional dos alunos, tendo como base o modelo de Educação Baseada em Resultados, onde os estudantes são avaliados de acordo com as metas atingidas e a qualidade das atividades realizadas. É realizada a implementação de uma versão inicial da solução, onde são registrados dados sobre as turmas, número de alunos, cursos, indicadores de desempenho, graus de desempenho e outras informações. Contudo, não são apresentados detalhes sobre a Blockchain utilizada no projeto.

De acordo com Bai et al. (2019), é possível ocorrer falsificações de documentos e adulterações de informações em projetos de pesquisa. Os autores propõem a criação de uma solução baseada em Blockchain para o gerenciamento e registro de todas as etapas de projetos de pesquisas. Nesta solução, cada agente envolvido na pesquisa possui um nó na Blockchain. Exemplos de agente incluem a agência financiadora, os pesquisadores, os auditores financeiros, dentre outros. Assim, todas as atividades desenvolvidas são registradas na Blockchain, passando pela validação do nó da agência financiadora. Dessa forma, descentralizando os dados, torna-se possível assegurar a sua imutabilidade e preservação. Contudo, o trabalho descreve apenas a modelagem da aplicação, não apresentando detalhes específicos acerca da sua implementação.

### 4.3 Utilizando *Smart Contracts* em ambientes acadêmicos

Nesta temática, Cheng et al. (2018) propõem o uso de *Smart Contracts* registrados em Blockchain para a emissão e validação de diplomas. No contrato serão definidas as condições necessárias para a conclusão do curso, o prazo disponível e outras informações. Quando o aluno cumprir todas as especificações, o contrato se auto executa e o diploma poderá ser emitido.

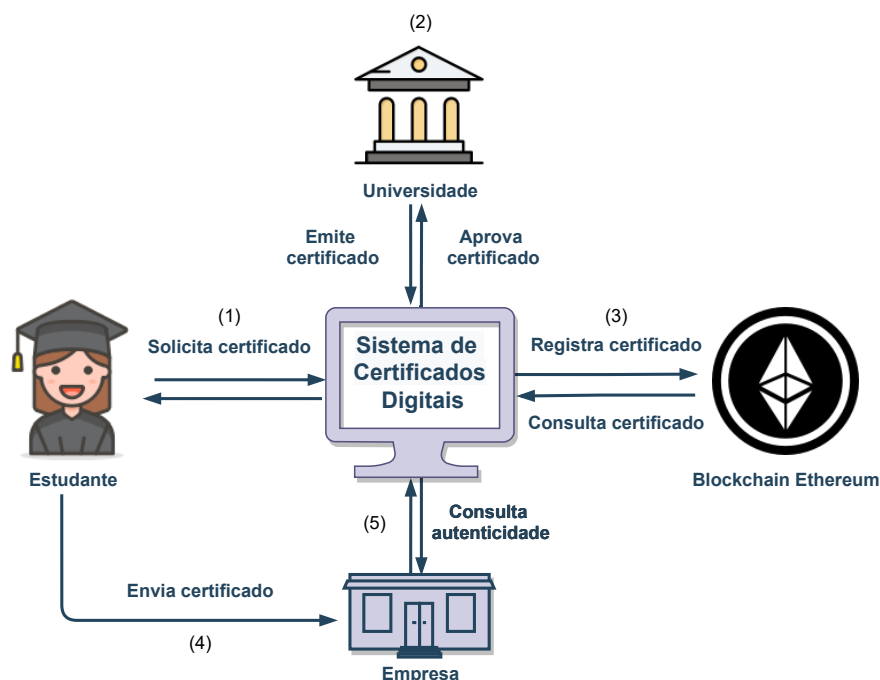
O trabalho descreve a modelagem e implementação de um sistema desenvolvido para a plataforma Ethereum utilizando a linguagem *Solidity*. É apresentado um exemplo de geração de um certificado e o seu registro na rede Ethereum mediante a criação de um *Smart Contract* contendo as suas informações. O sistema proporciona economia de papel, reduz custos de gerenciamento, evita a falsificação de documentos e fornece informações precisas e confiáveis sobre os certificados digitais emitidos.

A Figura 7 apresenta o fluxo de emissão de um certificado digital através da plataforma. O aluno pode realizar a solicitação do seu certificado através da plataforma (1). A universidade tem a função de inserir os dados do estudante no sistema e também de realizar a validação dos certificados emitidos (2). Uma vez que o arquivo é gerado, o seu *hash* é calculado e registrado na Blockchain (3), ficando o seu número impresso em uma etiqueta que será afixada na versão impressa do documento, caso esta seja solicitada pelo aluno. Desta forma, o sistema não apenas aumenta a credibilidade dos certificados que são emitidos em papel como também reduz eletronicamente os riscos de perda ou dano destes documentos.

De posse do seu certificado, o aluno poderá enviar o mesmo a outras entidades, como empresas empregadoras (4), que poderão, por sua vez, consultar a autenticidade das informações descritas no documento (5).

Ocheja, Flanagan e Ogata (2018) propõem a criação de um sistema de avaliação de aprendizagem baseado em Blockchain. A solução proposta realiza o acesso as bases

Figura 7 – Fluxo de emissão de um certificado digital utilizando Blockchain Ethereum.



Fonte: O autor (2021).

de dados dos alunos, reúne suas principais informações (ex.: notas, avaliações, dados comportamentais, etc.) e organiza tais informações na forma de *Smart Contracts*, que serão enviadas à rede Blockchain Ethereum. Tais contratos se auto executarão na medida em que o aluno progride no curso, garantindo assim o registro de todas as suas atividades e interações na cadeia de blocos. Isto permite uma maior interoperabilidade entre as bases de dados educacionais, garantindo o registro de dados de forma imutável e fará com que o acesso às informações ocorra de forma segura.

Também é possível a utilização de *Smart Contracts* para a realização de pagamentos. Rooksby e Dimitrov (2017) propõem a criação de uma plataforma baseada em Blockchain Ethereum para utilização em ambientes universitários. Esta proposta permite o registro de alunos e de suas respectivas notas nos cursos. Na plataforma existe uma criptomoeda, chamada *Kelvin Coin*, que o estudante recebe como recompensa mediante o bom desempenho nas atividades acadêmicas. Com a moeda o aluno poderá pagar por seus novos cursos mediante a execução de *Smart Contracts*.

Outro trabalho de pesquisa é apresentado por Gilda e Mehrotra (2018), que afirmam ser possível utilizar *Smart Contracts* para gravar as informações de consentimento dos envolvidos em uma pesquisa e permitir que essas informações sejam monitoradas com facilidade e transparência e possam ser revogadas caso necessário. Os autores descrevem a modelagem de um sistema, implementado na plataforma *Hyperledger Fabric*, para a criação e gravação destes registros na Blockchain. Os dados dos estudantes são adquiridos por meio de voluntários, que se reúnem pessoalmente com eles, e, através do preenchimento

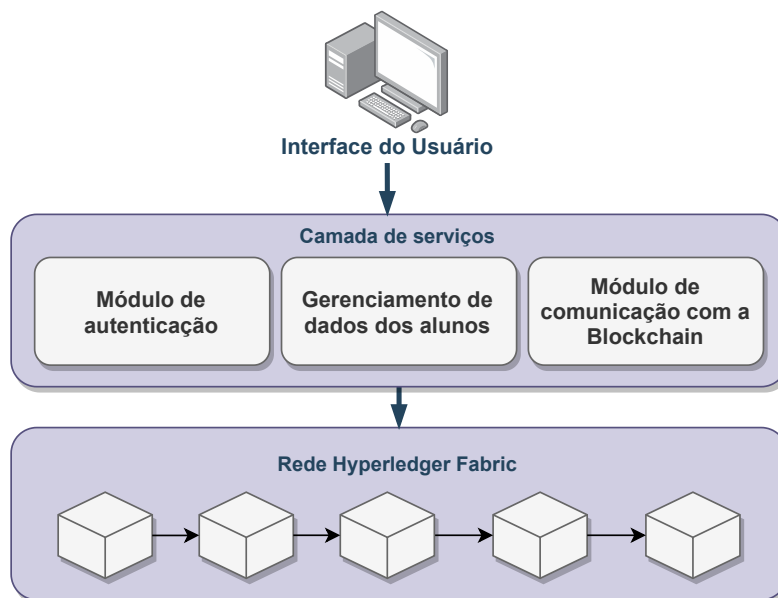
de formulários, obtêm as informações. Em seguida, os dados são registrados na Blockchain, permitindo assim o seu acesso por todos os envolvidos na pesquisa mediante a utilização de suas credenciais de acesso.

## 4.4 Registrando o conhecimento em Blockchain

Liu et al. (2018) sugere o uso de Blockchain para o registro de informações geradas pelos estudantes através da criação de uma plataforma distribuída que trará transparência, segurança e integridade aos dados. O trabalho apresenta a modelagem da solução fazendo uso da plataforma *Hyperledger Fabric*.

O protótipo do sistema utiliza dois nós de *Hyperledger* e serve para registrar as diferentes informações relacionadas a cada aluno, como suas notas, histórico escolar, atividades desenvolvidas, dentre outras. São armazenadas informações não apenas da instituição de ensino atual onde o aluno se encontra, mas também de todos os demais lugares por onde ele passou, devido à interoperabilidade permitida pela Blockchain. A Figura 8 apresenta a arquitetura da aplicação e suas diferentes camadas. O sistema possui diversos módulos com finalidades específicas, como autenticação, gerenciamento dos dados dos alunos e acesso aos nós da Blockchain.

Figura 8 – Visão geral da proposta descrita por Liu et al. (2018).



Fonte: O autor (2021).

Sharples e Domingue (2016), por sua vez, propõem um sistema de reputação acadêmica, fazendo uso de uma Blockchain privada baseada em Ethereum. Nesta Blockchain os alunos recebem uma moeda virtual chamada *Kudos* como prova dos créditos, trabalhos desenvolvidos ou conquistas obtidas. Os *Kudos* podem ser negociados, vendidos e trocados dentro das instituições de ensino. Um sistema de reputação como este apresenta benefícios

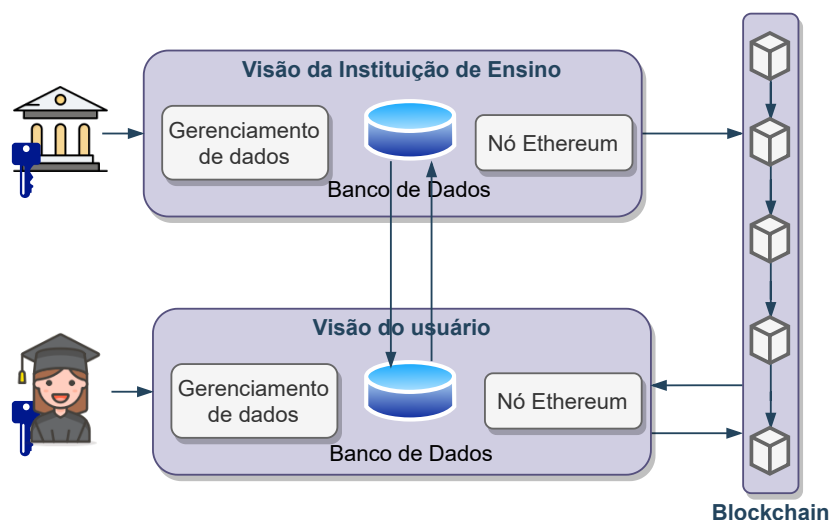
para as instituições como, por exemplo, fornecer um registro seguro, acessível e distribuído da escolaridade dos alunos. Através da utilização de uma Blockchain educacional, os indivíduos e instituições poderão armazenar registros públicos de realizações pessoais de forma confiável e facilmente verificável.

Em seu trabalho, Zhong et al. (2019) apresentam o projeto de uma plataforma que serve para registrar os alunos e armazenar as informações de todas as suas atividades acadêmico/escolares. O sistema possui mecanismos de recompensa que premiam o aluno, em criptomoedas, pelas conquistas alcançadas. Essas moedas podem ser usadas para compra de materiais de estudo, o que ajuda inclusive a evitar plágio e proteger a propriedade intelectual dos proprietários.

A plataforma é desenvolvida em NodeJs e realiza o registro dos dados em um banco de dados MongoDB, a partir de onde são enviados à Blockchain. A cadeia de blocos é constantemente monitorada, e desta forma é feito o acompanhamento do progresso de aprendizagem do aluno até que este chegue ao término do curso e o seu certificado possa ser emitido.

Han et al. (2018) propõem a criação de uma plataforma baseada em Ethereum que permite a instituição de ensino registrar todos os seus alunos e suas trajetórias acadêmicas, assim como o conhecimento produzido por cada indivíduo. Esta plataforma viabiliza também o registro de diplomas e certificados, que poderão ser validados sempre que necessário, por qualquer interessado, seja outra instituição de ensino ou empregadores. A Figura 9 apresenta a arquitetura da aplicação. Na parte superior está representado o módulo de visão da instituição, onde é possível realizar a inserção e atualização dos dados dos estudantes, que serão gravados na rede Ethereum. Na parte inferior da figura, encontra-se o módulo do usuário, onde é possível acessar os dados.

Figura 9 – Representação do funcionamento da aplicação.



Fonte: O autor (2021).

Coelho e Brandão (2019) buscam solucionar problemas que existem em bases de registro de pesquisa científica, como por exemplo falsificações, adulterações e plágios. O trabalho propõe a criação de uma solução baseada em Blockchain para o gerenciamento e registro de todas as etapas dos projetos de pesquisas, especialmente as publicações. Nela, os autores podem submeter os seus trabalhos de forma gratuita, e com a garantia de autenticidade fornecida pela Blockchain. Os revisores receberão os trabalhos e os avaliarão, de forma anônima e descentralizada. Por se tratar de um sistema descentralizado, não poderão ocorrer monopólios ou qualquer outra forma de controle por grupos de indivíduos com interesses especiais. A aplicação proposta recompensa os autores e revisores dos periódicos com um *token* digital que eventualmente pode ser trocado por criptomoedas.

## 4.5 Avaliação comparativa dos trabalhos

No Quadro 1 é apresentado um comparativo entre todos os trabalhos relacionados descritos nesta pesquisa. As segunda coluna deseja verificar se o trabalho apresenta implementação prática de soluções utilizando Blockchain; na terceira coluna é observado se o artigo faz uso de Blockchains públicas ou privadas, e se sim, qual delas; na quarta coluna é analisado se o trabalho descreve recursos de integração de Blockchains a sistemas legados; na quinta coluna é observado se o artigo propõem recursos para integração de AVAs a Blockchain.

Quadro 1 – Comparativo dos trabalhos relacionados.

| Trabalhos                                       | Apresenta implementação prática? | Usa Blockchain pública ou privada? | Possui recursos para integração de Blockchain a sistemas legados? | Propõe recursos para integrar Blockchain a ambientes educacionais? |
|-------------------------------------------------|----------------------------------|------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------|
| Al Harthy, Al Shuhaimi e Juma Al Ismaili (2019) | Não                              | Não Informada                      | Não                                                               | Não                                                                |
| Kolvenbach, Ruland e Gräther (2018)             | Sim                              | Pública (Ethereum)                 | Não                                                               | Não                                                                |
| Huynh et al. (2018)                             | Sim                              | Privada                            | Não                                                               | Não                                                                |
| Kanan, Obaidat e Al-Lahham (2019)               | Sim                              | Pública (Ethereum)                 | Não                                                               | Não                                                                |
| Arenas e Fernandez (2018)                       | Sim                              | Pública (Ethereum)                 | Não                                                               | Não                                                                |
| Srivastava et al. (2019)                        | Sim                              | Privada                            | Não                                                               | Não                                                                |
| Bore et al. (2017)                              | Sim                              | Pública (Hyperledger)              | Não                                                               | Não                                                                |
| Holbl et al. (2018)                             | Sim                              | Pública (Ethereum)                 | Não                                                               | Não                                                                |
| Turkanović et al. (2018)                        | Sim                              | Pública                            | Não                                                               | Não                                                                |
| Mikroyannidis et al. (2019)                     | Não                              | Pública (Ethereum)                 | Não                                                               | Não                                                                |
| Duan, Zhong e Liu (2018)                        | Sim                              | Não Informada                      | Não                                                               | Não                                                                |
| Bai et al. (2019)                               | Não                              | Não Informada                      | Não                                                               | Não                                                                |
| Cheng et al. (2018)                             | Sim                              | Pública (Ethereum)                 | Não                                                               | Não                                                                |
| Ocheja, Flanagan e Ogata (2018)                 | Não                              | Pública (Ethereum)                 | Sim                                                               | Sim                                                                |
| Rooksby e Dimitrov (2017)                       | Sim                              | Pública (Ethereum)                 | Não                                                               | Não                                                                |
| Gilda e Mehrotra (2018)                         | Sim                              | Pública (Hyperledger)              | Não                                                               | Não                                                                |
| Liu et al. (2018)                               | Sim                              | Pública (Hyperledger)              | Não                                                               | Não                                                                |
| Sharples e Domingue (2016)                      | Sim                              | Privada                            | Não                                                               | Não                                                                |
| Zhong et al. (2019)                             | Sim                              | Não Informada                      | Não                                                               | Não                                                                |
| Coelho e Brandão (2019)                         | Não                              | Não Informada                      | Não                                                               | Não                                                                |
| Jing Selenia e Han (2018)                       | Sim                              | Pública (Ethereum)                 | Não                                                               | Não                                                                |

Fonte: O autor (2021).

De acordo com a tabela, é possível perceber que a maioria dos trabalhos apresenta algum tipo de implementação prática de solução, que faz uso de Blockchain para o registro



de dados educacionais. Grande parte dos autores fazem uso de Blockchains públicas (Ethereum ou Hyperledger), alguns trabalhos apresentam apenas modelos conceituais, por isso não mencionam implementações ou o uso real de Blockchains. Também foi avaliado se os trabalhos apresentam recursos para integração de Blockchain a sistemas legados e a ambientes educacionais de aprendizagem, destes apenas um menciona estas funcionalidades, porém não faz menção ao AVA Moodle, nem descreve detalhes de implementação.

A solução proposta neste trabalho de dissertação difere-se das demais, pois propõe recursos de integração do AVA Moodle a Blockchain Ethereum e descreve detalhes de implementação. Os conceitos apresentados nesta solução poderão ser utilizados também para realizar a integração de outros AVAs a outras Blockchains.

## 4.6 Desafios de pesquisa em aberto

Após a avaliação dos trabalhos apresentados neste capítulo, foi possível identificar pontos que ainda precisam ser melhor aprofundados pela comunidade científica. São eles:

- **Avaliação da melhor arquitetura a ser usada para Blockchains com fins educacionais.** Em uma Blockchain pública tem-se acesso a uma rede verdadeiramente descentralizada, onde todos os nós podem armazenar uma cópia da cadeia de blocos ou atuar como mineradores. Em uma rede privada, existe a presença de um órgão regulamentador, seja uma pessoa ou um grupo, o que torna a rede centralizada ou permissionada. Para participar da rede é necessário obter um convite ou autorização e cumprir todas as regras, condições e políticas definidas pelo órgão regulador. Todos estes fatores devem ser avaliados quando da escolha de uma Blockchain pública ou privada, e um estudo mais aprofundado sobre esta temática se faz necessário.
- **Avaliação de desempenho, segurança e custos de Blockchains com fins educacionais.** Caso a instituição de ensino opte por implementar uma rede Blockchain local, dentro da infraestrutura do campus, é necessário avaliar se essa nova camada de segurança irá ocasionar alterações significativas no desempenho da rede e do sistema educacional. Também é importante analisar se o nível de segurança apresentado por tal aplicação será satisfatório, através de uma avaliação de segurança, levando em consideração todas as variantes envolvidas. Caso seja utilizada uma Blockchain pública, é necessário avaliar o custo de registro de cada documento.
- **Integração de Blockchain a sistemas legados.** É preciso avaliar maneiras de integrar as redes Blockchain aos sistemas legados e bases de dados já existentes e em uso nas universidades e instituições de ensino. Atualmente a maioria das instituições já faz uso de plataformas de registro, onde são armazenados os dados dos alunos. No

entanto, integrar tais sistemas com uma rede Blockchain pode ser um desafio devido à diversidade de tecnologias utilizadas em cada caso.

- **Ferramentas de suporte à integração de Blockchain com ferramentas da área de Informática na Educação.** Atualmente, os avanços da Informática na Educação são muito relevantes e vêm sendo amplamente adotados pela comunidade. O uso de tecnologias de suporte a EAD (como AVAs e ferramentas de videoconferência) se tornam cada vez mais frequentes. Neste contexto, existe o desejo de que determinados requisitos de segurança sejam garantidos. Por exemplo, como verificar se uma atividade realmente foi entregue pelo aluno? Para isso, a integração destas ferramentas com Blockchain se mostra muito útil pois aumentará a confiabilidade das interações entre alunos e professores. No entanto, tal integração se mostra como um problema complexo, pois demanda a integração de diversos tipos de tecnologias e bases de dados diferentes.

## 4.7 Considerações finais

Neste capítulo foram apresentadas as principais pesquisas sobre o uso de Blockchain em contextos educacionais na atualidade. Muitas das propostas atuais se referem ao registro de diplomas e certificados, porém é possível perceber um crescente interesse da comunidade científica em aplicar a tecnologia Blockchain a outros âmbitos da educação, como na garantia de autenticidade de documentos acadêmicos, como históricos de notas, atividades avaliativas, dentre outras. Ainda neste capítulo foram descritas as propostas de uso dos *Smart Contracts* na educação, e como é possível registrar toda a trajetória de construção do conhecimento em Blockchain. Por fim, são apresentados os desafios de pesquisa ainda em aberto na área e que precisam ser levados em consideração ao utilizar a tecnologia na educação.

O próximo capítulo apresentará a solução proposta nesta dissertação, que visa contribuir nos desafios anteriormente citados, através da integração de Blockchain a um sistema legado, e a realização de avaliações de desempenho e custos financeiros da solução proposta.

## 5 BlockMoodle: Uma Solução para Integração de Ambientes Virtuais de Aprendizagem a Blockchain

Este capítulo apresenta o projeto e implementação da solução BlockMoodle, que tem o propósito de realizar a integração entre o Ambiente Virtual de Aprendizagem Moodle a Blockchain Ethereum. A plataforma Ethereum foi escolhida por ser uma das mais popularmente utilizadas atualmente, permitindo o registro de informações e a criação de *Smart Contracts*. A Seção 5.1 apresenta os requisitos funcionais e não funcionais do sistema. Na Seção 5.2 é apresentada uma visão geral da solução. A Seção 5.3 apresenta o desenvolvimento da BlockMoodle e suas principais funcionalidades. Por fim, na Seção 5.4 são apresentadas as considerações finais deste capítulo.

### 5.1 Definição dos requisitos

A definição de requisitos é uma das etapas mais importantes em um projeto de *software*, pois fornece mecanismos apropriados para a compreensão do problema e quais necessidades o sistema deverá atender, e assim ser possível propor formas de solução eficientes (PRESSMAN, 2009). Nesta seção são apresentados os requisitos funcionais e os requisitos não funcionais da solução proposta neste projeto.

#### 5.1.1 Requisitos funcionais

Os requisitos funcionais (RF) dizem respeito a recursos específicos da aplicação, suas funções e seus componentes, podendo ser comportamentos, manipulação de dados, dentre outras possibilidades. No Quadro 2, são apresentados os requisitos funcionais definidos para a BlockMoodle, que indicam as principais funcionalidades que o sistema apresenta.

Quadro 2 – Requisitos Funcionais da BlockMoodle.

| ID    | Nome                                                       |
|-------|------------------------------------------------------------|
| RF 01 | Consultar as informações na base de dados do Moodle        |
| RF 02 | Gerar relatórios em PDF                                    |
| RF 03 | Calcular o <i>hash</i> dos relatórios                      |
| RF 04 | Registrar os relatórios na Blockchain Ethereum             |
| RF 05 | Disponibilizar os documentos emitidos para <i>download</i> |
| RF 06 | Validar os documentos gerados pela aplicação               |

Fonte: O autor (2021).

Os requisitos, descritos na tabela, consistem na consulta por informações na base de dados do Moodle (sobre cursos, alunos, atividades, notas, etc), são estas informações que serão armazenadas posteriormente na Blockchain; geração de relatórios em PDF com as informações coletadas, estes documentos serão armazenados e disponibilizados ao aluno, como prova da formação recebida; cálculo do *hash* do documento gerado, este é um requisito muito importante, pois será o valor do *hash* que será registrado na Blockchain Ethereum; disponibilização do arquivo para *download*; e por fim deverá ser possível a validação dos documentos, onde o usuário deverá submetê-lo novamente ao sistema, que calculará novamente o seu *hash* e verificará se este se encontra registrado na Blockchain.

### 5.1.2 Requisitos não funcionais

Os requisitos não funcionais (RNF) dizem respeito à qualidade com que o sistema deve atuar. De acordo com Sommerville (2007) se não forem seguidos da forma correta podem causar o mau funcionamento do sistema. No Quadro 3 são apresentados os requisitos não funcionais da BlockMoodle.

Quadro 3 – Requisitos não funcionais da BlockMoodle.

| ID     | Nome                                                        |
|--------|-------------------------------------------------------------|
| RNF 01 | Integridade dos documentos registrados                      |
| RNF 02 | Escalabilidade da aplicação                                 |
| RNF 03 | Divisão arquitetural em camadas                             |
| RNF 04 | Não impor sobrecarga significativa de desempenho ao sistema |

Fonte: O autor (2021).

No quadro acima são apresentados os requisitos não funcionais da BlockMoodle. O primeiro deles diz respeito à integridade dos dados. O princípio da integridade assegura que os dados não sejam modificados ou apagados indevidamente. O registro em Blockchain garante a integridade dos dados pois estes são assinados através de chaves criptográficas assimétricas. No momento em que a carteira digital é gerada, o algoritmo cria duas chaves, uma privada que é propriedade exclusiva do usuário, e outra pública, que é distribuída na rede. As aplicações de tais chaves são diversas, servindo para verificar a autoria de uma mensagem, ou garantir a integridade criptografando o dado a ser enviado.

Na BlockMoodle os relatórios que contêm os dados pessoais dos alunos são criptografados e apenas a sua chave *hash* é registrada na Blockchain, sendo necessário que o usuário utilize a chave privada da sua carteira, que na aplicação é gerenciada pelo Metamask. No momento da validação de um documento, verifica-se se o *hash* do referido arquivo é igual ao que se encontra registrado no *Smart Contract*; em caso afirmativo é possível assegurar a integridade do documento, e que ele foi gerado pela aplicação.

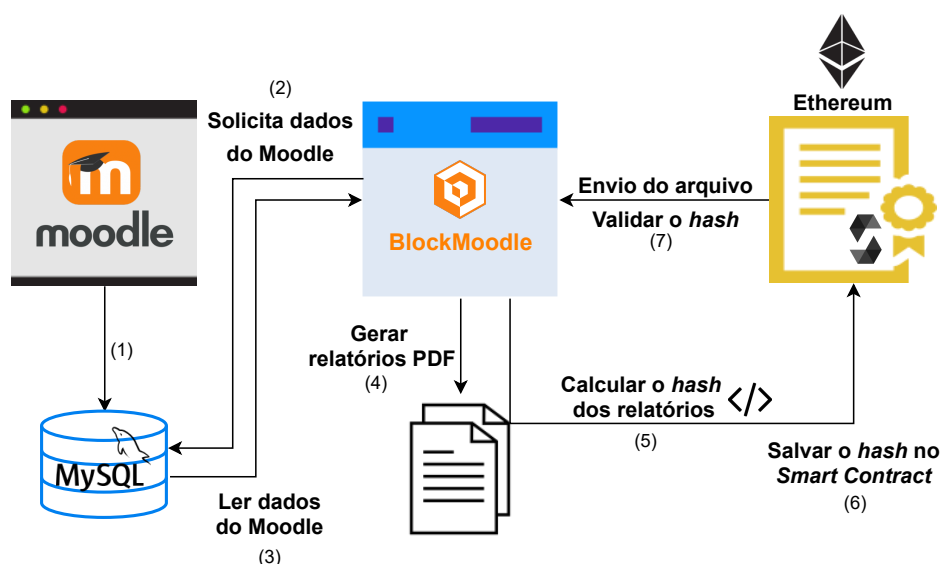
A aplicação deve ainda ser escalável, permitindo assim, que um grande número de requisições sejam atendidas, sem que isso aumente drasticamente o consumo de recursos;

o sistema deverá ser dividido em camadas para facilitar a sua manutenção, aumentando assim a coesão e reduzindo o acoplamento. Outro requisito desejável é que a solução não imponha uma sobrecarga significativa de desempenho ao sistema, isto é, que atenda uma grande quantidade de usuários em tempo hábil.

## 5.2 Visão Geral

A Figura 10 ilustra o funcionamento da aplicação, e como se dá a integração entre o Moodle e a ferramenta BlockMoodle.

Figura 10 – Visão geral do funcionamento da BlockMoodle.



Fonte: O autor (2021).

O Moodle realiza o registro de todos os seus dados em um banco de dados relacional MySQL (1). Em uma estrutura interna de tabelas são registradas as informações referentes a diversos aspectos, como cursos, atividades, notas e informações sobre os usuários e as interações que ocorrem entre eles através dos fóruns e chats.

A BlockMoodle realiza o acesso à base de dados do Moodle, onde são coletados os dados, através de consultas SQL, e que serão escolhidos pelo usuário para serem registrados na Blockchain (2), como informações pessoais dos alunos, os cursos em que estes se encontram matriculados, as atividades realizadas e suas respectivas notas. O usuário responsável pela emissão de documentos na BlockMoodle será um funcionário da instituição de ensino, que decidirá qual documento será gerado de acordo com as demandas da instituição ou a solicitação do aluno, por exemplo um histórico de notas.

No Quadro 4 são apresentadas as tabelas do Moodle que são acessadas pela BlockMoodle, elas contêm os dados necessários para a emissão dos documentos. Caso novas

funcionalidades sejam integradas a BlockMoodle posteriormente, novas tabelas poderão ser escolhidas para acesso.

Quadro 4 – Tabelas do Moodle acessadas pelo BlockMoodle para coleta de dados.

| Informações | Tabelas do Moodle                                                                  |
|-------------|------------------------------------------------------------------------------------|
| Alunos      | mdl_user                                                                           |
| Notas       | mdl_grade, mdl_grade_grades, mdl_grade_items                                       |
| Cursos      | mdl_course, mdl_course_categories, mdl_role_assignments, mdl_context               |
| Atividades  | mdl_quiz, mdl_forum, mdl_resource, mdl_choice, mdl_url, mdl_glossary, mdl_feedback |

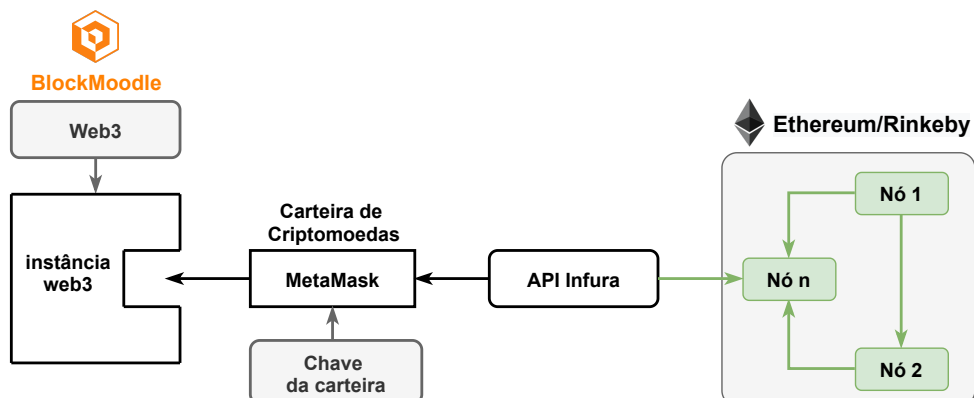
Fonte: O autor (2021).

Todas estas informações serão organizadas em relatórios no formato PDF (3), por ser um padrão amplamente difundido para o intercâmbio de documentos, para em seguida serem registrados na Blockchain. Os documentos gerados serão disponibilizados ao solicitante e permanecerão armazenados no servidores da BlockMoodle.

Após a criação de um relatório, a aplicação faz o cálculo do seu *hash* (4). Para isto é utilizada a função de *hash* sha256, que recebe como entrada o arquivo do relatório e retorna uma *string* de 64 bits, que corresponde ao valor do *hash* do documento. Esta *string* é uma representação numérica do arquivo correspondente. Em seguida o *hash* do arquivo será enviado ao *Smart Contract* que se encontra registrado na Blockchain Ethereum (5).

Para realizar a comunicação da BlockMoodle com a Blockchain é utilizada a API Web3, que utiliza o formato JSON para a troca das informações necessárias com a plataforma Ethereum. A Figura 11 mostra um esquema de como acontece esta comunicação.

Figura 11 – Visão geral da integração da aplicação com a Ethereum.



Fonte: O autor (2021).

Conforme ilustra a Figura 11 é criada uma instância de Web3, responsável por realizar a comunicação com a carteira de criptomoedas Metamask, onde é verificado se há saldo suficiente para o registro do documento. Esta mesma instância se comunica também com a API Infura, que é responsável por interagir diretamente com a rede Ethereum.

Através da BlockMoodle é possível também realizar a validação dos relatórios. Para isto, é realizado o *upload* do arquivo, e o seu *hash* é calculado (6) através do uso da biblioteca sha256 0.2.0. Após esta etapa, realiza-se a consulta ao *Smart Contract* para verificar se o *hash* se encontra registrado na Blockchain.

## 5.3 Projeto e Implementação

Após a definição dos requisitos do sistema, realizou-se a implementação de suas funcionalidades principais. Esta seção detalha informações acerca do projeto e implementação da solução proposta nesta dissertação.

### 5.3.1 Ferramentas utilizadas

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

- **Solidity:** consiste em uma linguagem de programação orientada a objetos que permite escrever contratos inteligentes para diversas Blockchains, em especial a Ethereum. Neste projeto foi utilizada para a criação do código fonte do *Smart Contract* da BlockMoodle.
- **React:** trata-se de uma biblioteca JavaScript, de código aberto, que permite a criação de interfaces de usuário em páginas Web de forma simples e eficaz. Foi utilizado em todo o projeto para a criação da interface visual, que permite o acesso às funcionalidades do sistema.
- **Web3.js:** funciona como uma API Javascript que permite realizar as conexões necessárias com a plataforma Ethereum, utilizando a especificação JSON. Com o uso dessa biblioteca foi possível realizar a comunicação entre o front-end da aplicação e um nó da Blockchain Ethereum.
- **Metamask:** consiste em uma carteira de criptomoedas que pode ser utilizada como uma extensão nos navegadores Chrome, Firefox e Brave. Tem a finalidade de funcionar como uma ponte entre os navegadores Web e a Blockchain Ethereum. Foi utilizada para o pagamento da taxa de registro de cada documento gerado pelo BlockMoodle na Blockchain Ethereum.

### 5.3.2 Implementação da solução BlockMoodle

Para o desenvolvimento desta solução realizou-se a instalação de uma instância local do ambiente Moodle 3.9.1, que por se tratar de um software livre está disponível

gratuitamente para *download*. Neste trabalho optou-se pelo uso da rede de testes Rinkeby<sup>1</sup>, que funciona de forma análoga à rede Ethereum, porém é possível executar os testes sem o gasto de Ether real, utilizando pseudo Ethers.

O registro dos dados na Blockchain é feito através de um *Smart Contract*, escrito na linguagem *Solidity 0.4.17*. A seguir é apresentado o código fonte do contrato implementado (Figura 12). Neste contrato é definida uma estrutura chamada *Report* (linha 4), que contém os principais dados que deverão ser registrados: a descrição do relatório; o *Timestamp* da sua criação; o endereço do criador do registro; o *hash* do relatório e o seu tipo.

O *Smart Contract* contém duas funções principais: *creatReport* (linha 17), que será invocada no momento da criação de um novo registro, e a função *getLength* (linha 28), que será útil no momento da validação de um relatório, pois permitirá percorrer a estrutura de dados e localizar o hash do documento que se deseja validar.

Figura 12 – Código fonte do *Smart Contract* utilizado pelo BlockMoodle.

```
1  pragma solidity ^0.4.17;
2
3  contract Moodle{
4
5      struct Report {
6          string description;
7          uint timestamp;
8          address sender;
9          string doc;
10         uint tipo;
11     }
12     address public manager;
13     Report[] public docs;
14     function Moodle() public {
15         manager = msg.sender;
16     }
17     function createReport(string memory description,
18         string memory valor, uint tipo) public {
19         Report memory newReport = Report({
20             description: description,
21             timestamp: now,
22             sender: msg.sender,
23             doc: valor,
24             tipo: tipo
25         });
26         docs.push(newReport);
27     }
28     function getLength() public view returns (uint) {
29         return docs.length;
30     }
31 }
```

Fonte: O autor (2021).

<sup>1</sup> <https://www.rinkeby.io>



Para a realização do registro é necessário o pagamento de uma taxa, criptomoeda Ether, a cada nova transação. Esta taxa é requerida pela Blockchain Ethereum devido aos custos de mineração necessários para validar cada bloco e os adicionar à cadeia.

Para a execução deste trabalho utilizou-se o Metamask, que se trata de uma carteira de criptomoedas, podendo ser utilizada como uma extensão dos navegadores Chrome, Firefox e Brave. O Metamask faz a integração entre a aplicação que está sendo executada nos navegadores e a Blockchain Ethereum.

Para ter acesso à solução BlockMoodle, o usuário deverá realizar login, informando e-mail e senha, conforme apresentado na Figura 13. Há dois tipos de privilégios de usuário: o administrador, que poderá ter acesso à base de dados no Moodle e realizar a criação de novos documentos, e o aluno, que poderá utilizar a plataforma apenas para consulta e validação dos documentos que dizem respeito a ele, como o seu histórico escolar, por exemplo.

Figura 13 – Tela de login da aplicação BlockMoodle.



Fonte: O autor (2021).

Após a inserção das informações corretas e realização bem-sucedida do login, o usuário será redirecionado para a tela inicial da aplicação, onde serão apresentadas as principais funcionalidades disponíveis, como validar ou gerar novos relatórios, conforme apresentado na Figura 14.

A partir desta tela, é possível visualizar e gerar novos relatórios de usuários, que contém os dados de todos os usuários cadastrados no Moodle; relatórios de cursos, que contém informações relevantes sobre os cursos ativos e inativos do AVA; históricos de notas, que poderão ser de toda a turma ou de um aluno específico; e também relatórios de todas as atividades disponíveis em um curso do Moodle.

Para a criação e exibição dos relatórios no formato PDF é utilizado o EJS, que se trata de uma biblioteca de visualização, cuja finalidade é permite transportar dados do

backend para o frontend da aplicação, e assim utilizar códigos em JavaScript no HTML das páginas.

Figura 14 – Módulos contendo as funcionalidades disponíveis na aplicação.



Fonte: O autor (2021).

Dentre os documentos que podem ser gerados pelo BlockMoodle estão os históricos de notas dos alunos. Na Figura 15 é possível visualizar a interface apresentada pela aplicação para a geração dos relatórios de notas, onde o usuário deverá informar o e-mail do aluno e clicar no botão “Gerar”.

Figura 15 – Interface de geração do histórico de notas do aluno.

## Relatório de Notas

### Gerar histórico do aluno

**Email:**

Email...

**Gerar**

**Dica:** Informe o email do aluno para a realização da consulta. Ao clicar em "Gerar" será gerado um arquivo PDF com os dados, mas para isso será necessário a realização do pagamento de uma taxa em Ether para que seja possível a inserção do relatório na Blockchain.

Fonte: O autor (2021).

Caso seja possível localizar os dados do aluno na base de dados a aplicação fará a

criação de um relatório em PDF com as informações, conforme exemplificado na Figura 16, mostrada abaixo.

Após a geração do relatório, o arquivo no formato PDF é disponibilizado para download; em seguida a BlockMoodle realiza o cálculo do *hash* do documento, que será enviado à Blockchain.

Figura 16 – Relatório de notas gerados pela BlockMoodle.



**UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO**  
CNPJ: 24.416.174/0001-06  
DEPARTAMENTO DE REGISTRO DIGITAL

---

**HISTÓRICO DE NOTAS**

Este relatório apresenta os dados do(a) aluno(a) José Daniel matriculado(a) no curso Conceitos básicos sobre Blockchain oferecido pela plataforma BlockMoodle.

**Dados pessoais**

| Nome        | Email                | Telefone        | Data de cadastro |
|-------------|----------------------|-----------------|------------------|
| José Daniel | josedaniel@gmail.com | (87)9 9999-0000 | 31/Jul/2020      |

**Cursos Matriculados**

| Curso                              | Sigla   | Data da matrícula |
|------------------------------------|---------|-------------------|
| Conceitos básicos sobre Blockchain | CBB2020 | 31/Jul/2020       |

**Notas**

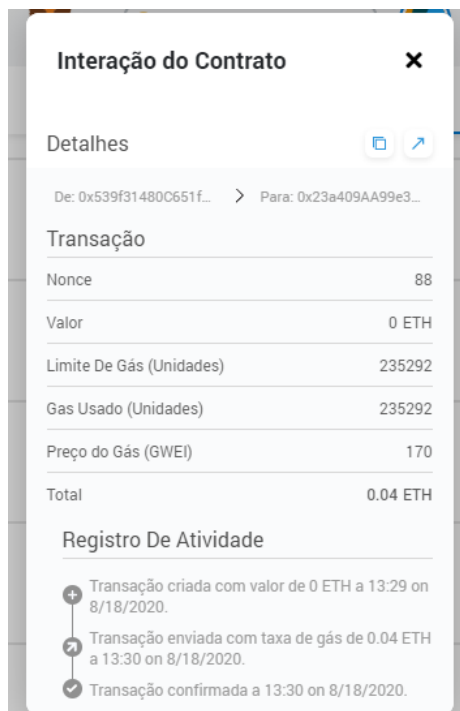
| Questionário | Glossário | Avaliação | Média |
|--------------|-----------|-----------|-------|
| 7.5          | 10.0      | 8.0       | 8.5   |

**RECIFE, 3/Mar/2021 às 10:39:51**

Fonte: O autor (2021).

Para que o registro na Blockchain seja realizado a aplicação solicitará o pagamento da taxa de mineração, que após confirmado efetivará o envio a Blockchain Ethereum. A Figura 17 mostra o pagamento de um relatório. Por fim o documento é disponibilizado para download.

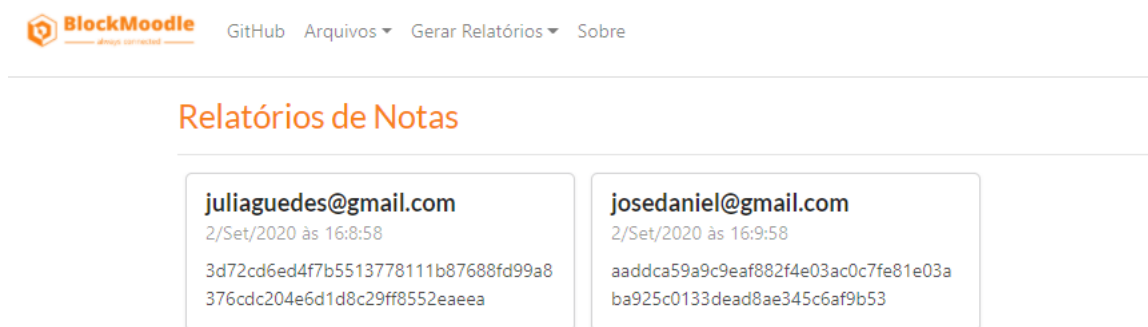
Figura 17 – Realização do pagamento para inclusão do relatório na Blockchain.



Fonte: O autor (2021).

Após a confirmação do pagamento o documento será registrado na Blockchain Ethereum, e uma mensagem de confirmação será apresentada ao usuário, junto com o download do documento solicitado. Na tela de relatórios é apresentado um resumo de todos os documentos que já foram gerados (Figura 18), contendo o *hash* do documento, o e-mail do estudante e a data e hora em que ocorreu o registro.

Figura 18 – Tela de resumo dos relatórios de notas.

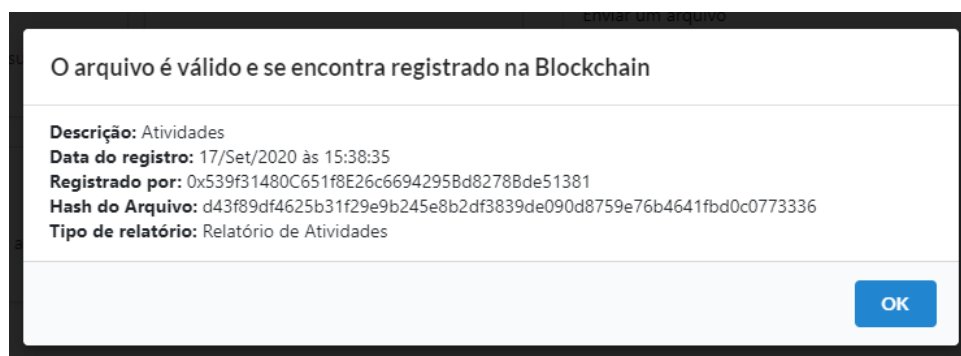


Fonte: O autor (2021).

Outra funcionalidade importante é a validação de relatórios. Para isso é necessário realizar o upload de um arquivo no campo disponibilizado na tela inicial. O arquivo é enviado ao backend via POST, em seguida o seu hash será calculado e o seu valor será consultado na Blockchain. Caso o mesmo seja válido e se encontre registrado na cadeia

de blocos, será exibida uma mensagem de confirmação. Esta mensagem contém os dados referentes ao documento, como a sua data de criação, o seu hash, o seu tipo, dentre outras informações relevantes, conforme apresentado na Figura 19.

Figura 19 – Mensagem de confirmação de autenticidade, exibida ao validar um documento.



Fonte: O autor (2021).

Caso o arquivo inserido não tenha sido gerado pela BlockMoodle, e, portanto, não se encontre registrado na Blockchain, será exibida uma mensagem de erro, informando ao usuário que o documento é inválido.

Para a realização de consultas na Blockchain não há a cobrança de taxas pela rede Ethereum, logo os alunos ou quaisquer interessados podem realizar validações de documentos sempre que houver necessidade sem a cobrança de taxas.

## 5.4 Considerações finais

Este capítulo apresentou o projeto e implementação da solução BlockMoodle, descrevendo as suas principais funcionalidades e o seu propósito de utilização. A ferramenta realiza a integração entre o Ambiente Virtual de Aprendizagem Moodle e a Blockchain Ethereum. Esta ferramenta realiza o acesso à base de dados do Moodle e coleta informações sobre cursos, atividades e notas, além de dados pessoais sobre os estudantes cadastrados. A solução proposta realiza a emissão de relatórios no formato PDF com as informações solicitadas, calcula o seu *hash* e, após o pagamento da taxa de mineração, realiza o registro dos documentos no *Smart Contract* que se encontra na rede Ethereum. Cada arquivo gerado pode ser validado através da própria plataforma, realizando novamente o cálculo do seu *hash* e consultando se aquele valor se encontra registrado no Blockchain.

Após o detalhamento da solução proposta, é importante fazer uma avaliação da mesma, e esta avaliação é o foco do próximo capítulo.



## 6 Avaliação

Este capítulo tem como objetivo avaliar a principal contribuição deste trabalho, a BlockMoodle. A Seção 6.1 apresenta uma análise do custo financeiro necessário para o registro de um novo relatório no *Smart Contract* BlockMoodle. Na Seção 6.2 é apresentada uma avaliação de desempenho para observar o comportamento da aplicação mediante a aplicação de diferentes cargas de trabalho. Na Seção 6.3 são apresentadas as considerações finais deste capítulo.

### 6.1 Avaliação de custos financeiros

Na Blockchain Ethereum existe um custo computacional associado à mineração de cada bloco. Logo, para incluir novos dados em um bloco, é necessário o pagamento de uma taxa. Este valor, medido em *Gwei*<sup>1</sup>, varia frequentemente, dependendo do nível de congestionamento da rede naquele instante. As transações que oferecem taxas maiores terão mais chances de serem escolhidas primeiro pelos algoritmos de mineração da Blockchain para entrar no bloco que será minerado.

O valor total da taxa de transação é dado por:

$$\text{Valor Total} = \text{Gas Limit} * \text{Gas Price} \quad (1)$$

Nesta equação, *Gas Limit* corresponde à quantidade total de *Gas*<sup>2</sup> que a transação poderá consumir. Este valor depende da operação que será realizada no *Smart Contract*. A cada instrução de código, processada pelo compilador da linguagem *Solidity*, é associado um custo necessário para a execução na Blockchain. Os custos adotados nas operações da rede Ethereum foram definidos pelo Ethereum Project Yellow Paper (WOOD et al., 2014).

Para o código da BlockMoodle é associado um custo de execução *Gas Limit* igual a 174000. Este valor foi obtido através de observações empíricas das execuções do Metamask, realizadas no contexto desta dissertação, onde após cada novo registro na Blockchain observou-se que este número se repete.

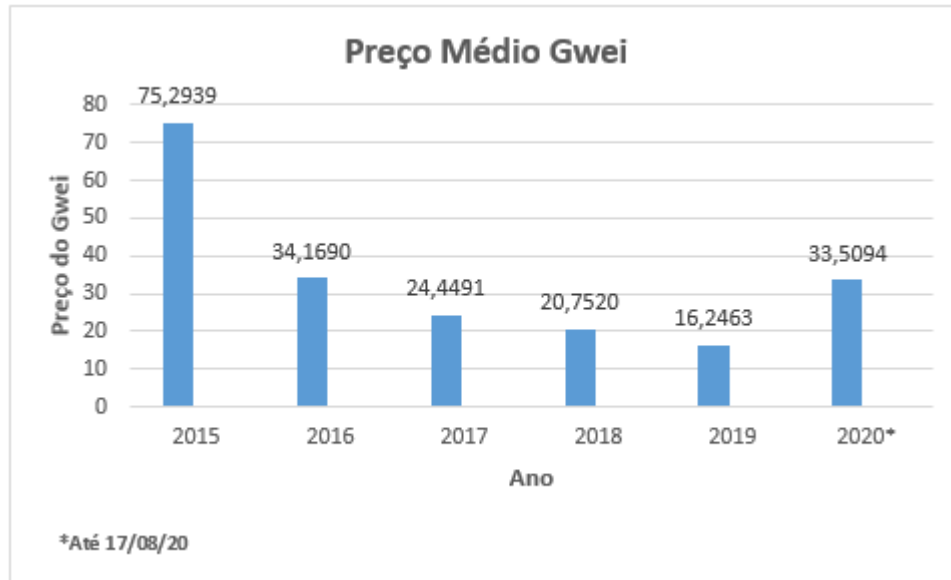
O valor do *Gas Price* varia de acordo com a quantidade de transações que estiverem sendo incluídas na Blockchain a cada momento. As médias diárias do preço do Gás é disponibilizada pela plataforma Etherscan.io (TEAM, 2017), onde são apresentados os valores desde o início da operação da rede, em Agosto de 2015, até Agosto de 2020.

<sup>1</sup> 1 *GWEI* corresponde a uma fração de 0.000000001 da criptomoeda Ether.

<sup>2</sup> Valor cobrado cada vez que uma transação ou contrato inteligente são executados no Ethereum.

Com o objetivo de mensurar o custo de inclusão de um relatório gerado pela BlockMoodle, neste trabalho obteve-se uma planilha com todos os valores diários de *Gas* (TEAM, 2017) e realizou-se o cálculo da média anual do *Gas Price*, cujos valores são apresentados na Figura 20. Por exemplo, o valor médio do preço do *Gas* no ano de 2019 foi de \$16,24 *Gwei*.

Figura 20 – Preço médio histórico anual do *Gwei*.



Fonte: O autor (2021).

Com estas informações é possível realizar uma estimativa de custo do BlockMoodle, e realizar um comparativo ano a ano do quanto custaria a geração de cada relatório ao longo do tempo. Utilizando a equação (1), temos que, para o ano de 2019, por exemplo, considerando o *Gas Limit* de 174000 e o preço médio do *Gwei* naquele ano de 0,0000000162463 (convertido para Ether), o custo seria de:

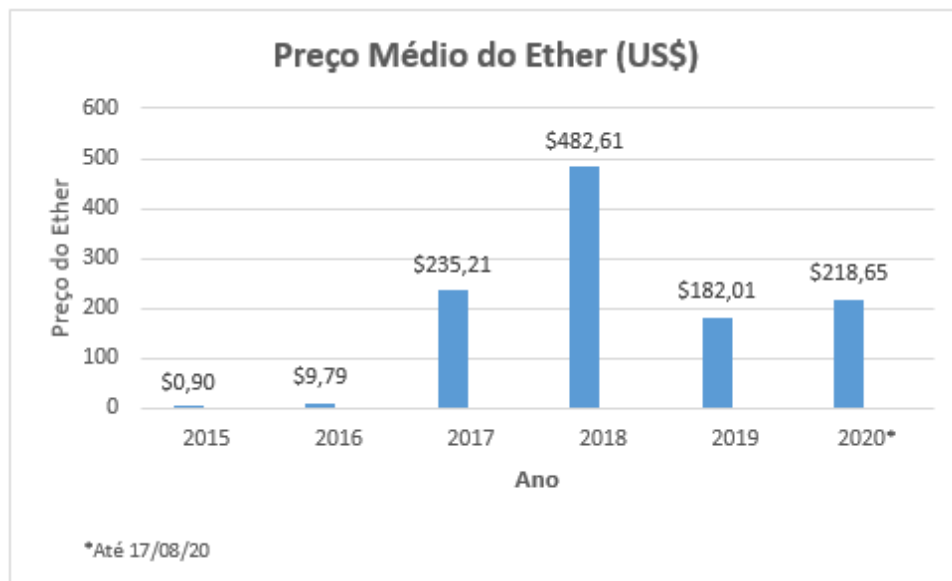
$$Total = 174000 * 0,0000000162463 = 0,0028268 \text{ Ether} \quad (2)$$

Assim, o custo necessário para inclusão de um relatório na Blockchain, em 2019, seria de 0.0028268 Ether. Para uma melhor análise, o preço do Ether pode ser convertido para dólar. Como a cotação do preço do Ether sofre constantes alterações, a depender das condições de mercado e de outros fatores, realizou-se um processo semelhante ao anterior, de cálculo médio do preço do Ether em dólar ano a ano (Figura 21). Por exemplo, no ano de 2019 o preço médio do Ether foi de U\$ 182,01 dólares. Multiplicando este valor pelo número obtido na equação (2), obtém-se que o custo naquele ano seria de U\$ 0,51 dólar.

Na Tabela 1 é feito um comparativo dos custos no decorrer dos anos, desde Agosto de 2015, no início da rede Ethereum, até Agosto de 2020. É possível perceber que o valor



Figura 21 – Preço médio histórico anual do Ether em Dólar.



Fonte: O autor (2021).

total sofreu diversas oscilações ao longo do tempo, partindo de U\$ 0,01 em 2015, chegando ao valor mais alto em 2018, quando atingiu U\$ 1,74.

Tabela 1 – Comparativo de custos ano a ano.

| Ano  | Gas Limit | Gas Price (Ether) | Total (Ether) | Total (US\$) |
|------|-----------|-------------------|---------------|--------------|
| 2015 | 174000    | 0,00000007529     | 0,0131        | \$ 0,01      |
| 2016 | 174000    | 0,00000003416     | 0,0059        | \$ 0,06      |
| 2017 | 174000    | 0,00000002444     | 0,0042        | \$ 1,00      |
| 2018 | 174000    | 0,00000002075     | 0,0036        | \$ 1,74      |
| 2019 | 174000    | 0,00000001624     | 0,0028        | \$ 0,51      |
| 2020 | 174000    | 0,00000003350     | 0,0058        | \$ 1,27      |

Fonte: O autor (2021).

Diante dos dados apresentados, caberá a cada instituição de ensino avaliar a viabilidade financeira da utilização da solução BlockMoodle, ou optar pela utilização de uma Blockchain privada, que seria implementada na própria instituição e não demandaria o pagamento de taxas. Ao optar pelo uso de Blockchain pública, a instituição deverá estar atenta ao fato de que os seus custos sofrerão alterações constantes devido as variações de cotação da criptomoeda Ether e do dólar.

## 6.2 Avaliação de desempenho da BlockMoodle

Esta seção apresenta a avaliação de desempenho realizada sobre a aplicação BlockMoodle, com o intuito de observar o seu comportamento mediante a aplicação de diferentes cargas de trabalho.

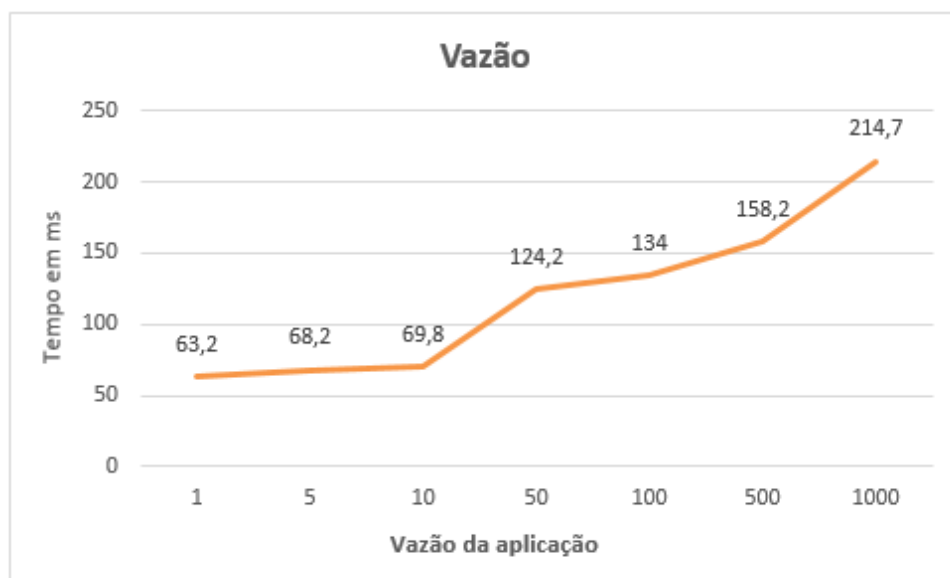
Para realizar a avaliação de desempenho de um sistema, é possível utilizar diferentes técnicas (YADAV; SOUSA; CALLOU, 2018; JAIN, 2008), dentre elas a medição, que faz a análise diretamente sobre o sistema real, aplicando diferentes cargas de trabalhos para mensurar o seu desempenho através das métricas coletadas. Na medição, utilizam-se ferramentas de *benchmark*, que permitem ao pesquisador a definição de parâmetros, como número de usuários simultâneos, e assim aproximar os resultados de uma situação de uso do mundo real.

Os parâmetros escolhidos para a análise do BlockMoodle foram a vazão, que corresponde à taxa na qual as requisições são atendidas pelo sistema, e o tempo de resposta, que é o tempo decorrido entre o início e a conclusão de um serviço (MENASCE et al., 2004). Foram aplicadas diferentes cargas de trabalho, que simulam diferentes quantidades de usuários realizando acessos simultâneos à aplicação. As cargas aplicadas foram de 1, 5, 10, 50, 100, 500 e 1000 acessos simultâneos.

Os testes foram realizados em uma máquina com processador Intel Core i5-10210U de 1,60GHZ, com 8GB de memória RAM. Foi utilizada a ferramenta JMeter, que permite definir a quantidade de acesso simultâneos que se deseja simular. Neste experimento, cada um dos acessos realiza uma requisição HTTP do tipo GET, simulando um usuário acessando a aplicação.

A Figura 22 apresenta o gráfico da vazão da solução para as quantidades de requisições simultâneas aplicadas. É possível perceber que conforme a quantidade de acessos simultâneos aumenta, o tempo de vazão necessário para atender a todas as requisições também aumenta.

Figura 22 – Vazão da aplicação BlockMoodle para diferentes quantidades de acessos simultâneos.



Fonte: O autor (2021).

A segunda métrica considerada foi a de tempo de resposta. A Figura 23 apresenta os resultados obtidos no experimento. Conforme o número de usuários simultâneos aumenta, cresce também o tempo de resposta da aplicação. Para o exemplo contendo 100 acessos, o tempo total de resposta foi de 773 milissegundos.

Figura 23 – Tempo de resposta da BlockMoodle para diferentes quantidades de acessos simultâneos.



Fonte: O autor (2021).

Na Figura 23 é possível perceber que há um crescimento considerável do tempo de resposta a partir de 100 usuários simultâneos. Assim, em casos onde haja uma quantidade de acessos simultâneos inferior a este número não serão notadas variações significativas do tempo de resposta.

Os valores do tempo de vazão e do tempo de resposta são considerados aceitáveis. Para 1000 acessos simultâneos, por exemplo, o tempo de vazão em milissegundos foi de 214,7, o que equivale a 0,2 segundo. Para até 100 acessos simultâneos, o tempo de resposta foi de 773 milissegundos, ou 0,7 segundo. De acordo com Miller (1968), tempos de espera entre 0,1 e 1 segundo são considerados toleráveis e não causa desvio de atenção na tarefa que está sendo realizada pelo usuário.

A utilização da solução BlockMoodle não tratá impacto de desempenho ao Moodle, pois realiza apenas consultas a sua base de dados. Nenhum dado é inserido ou modificado nas tabelas do Moodle.

## 6.3 Considerações finais

Este capítulo teve o propósito de avaliar a aplicação BlockMoodle em aspectos específicos. Inicialmente foi realizada uma avaliação de custos, para mensurar o quanto

será gasto para a geração de cada relatório pela plataforma. Depois, foi feita avaliação de desempenho para observar o comportamento de métricas como a vazão e o tempo de resposta da BlockMoodle em diferentes cenários de uso, através da aplicação de diferentes cargas de trabalho.

## 7 Conclusões e Trabalhos Futuros

Neste capítulo são descritas as conclusões e trabalhos futuros desta dissertação. Na Seção 7.1 são apresentadas as conclusões acerca da criação da ferramenta BlockMoodle e do uso de Blockchain para o registro de dados de uma Ambiente Virtual de Aprendizagem. Na Seção 7.2 são apresentadas as contribuições científicas deste trabalho. Na Seção 7.3 são descritas as possibilidades de trabalhos futuros a serem realizados como complemento a esta pesquisa.

### 7.1 Conclusões

Este trabalho teve como objetivo apresentar uma proposta de integração do Ambiente Virtual de Aprendizagem Moodle à Blockchain Ethereum, através da criação da ferramenta BlockMoodle. Inicialmente foi realizada uma pesquisa bibliográfica, com o intuito de conhecer o funcionamento da tecnologia Blockchain e dos *Smart Contracts*. Foi feito um levantamento do estado da arte sobre o uso de Blockchain em contextos educacionais, o que permitiu perceber a falta de propostas voltadas especificamente ao ensino a distância.

A tecnologia Blockchain se apresenta como uma tendência de inovação em diversas áreas, dentre elas a educação, devido ao potencial de segurança, confidencialidade, integridade e disponibilidade apresentados. É possível fazer uso desta tecnologia também na educação a distância, modalidade que vem crescendo cada vez mais e ganhando adeptos no mundo todo. A ferramenta BlockMoodle, apresentada neste trabalho, pode ser utilizada para diversos propósitos, como o registro seguro dos dados educacionais e garantia de autenticidade de documentos acadêmicos. O AVA Moodle foi escolhido por ser um dos mais populares e utilizados na EAD do mundo todo.

A BlockMoodle realiza o acesso à base de dados do Moodle e gera relatórios em PDF, contendo diversos dados dos cursos e seus respectivos alunos, bem como de suas notas e informações acadêmicas. Em seguida é calculado o *hash* dos relatórios e o registro em um *Smart Contract* na Blockchain Ethereum. Estes registros asseguram um maior nível de confiança e credibilidade aos dados, pois permanecerão gravados de forma imutável na cadeia de blocos e poderão ser verificados sempre que necessário.

A proposta descrita neste trabalho trouxe avanços ao estado da arte, pois apresenta uma solução que permite a integração entre um ambiente virtual de aprendizagem e uma Blockchain. Esta solução permitirá o registro seguro de dados da educação a distância, e possibilitará a verificação confiável destes dados, devido ao registro imutável na Blockchain.

Por fim, foi realizada uma avaliação de custo, que apresenta o valor a ser pago pelo registro de cada relatório na Blockchain; caberá às instituições de ensino que adotarem a proposta avaliar se o custo de registro da rede Ethereum está de acordo com os seus orçamentos. Realizou-se também uma avaliação de desempenho, que aponta o tempo de resposta e a vazão da ferramenta diante da aplicação de diferentes cargas de trabalho, que simulam cenários de uso distintos; os testes realizados apontam bons resultados da solução para quantidades de acessos simultâneos inferiores a 100 usuários.

## 7.2 Contribuições

A principal contribuição científica apresentada por este trabalho é a solução BlockMoodle, que realiza a integração entre o ambiente virtual de aprendizagem Moodle e a Blockchain Ethereum. Este trabalho mostrou ser possível o registro seguro de dados educacionais e documentos acadêmicos gerados pela educação a distância, utilizando Blockchain. É possível ainda, utilizar os conceitos apresentados por esta pesquisa para realizar a integração de outros AVAs a outras Blockchains.

Esta dissertação apresentou também outras contribuições relevantes, como uma revisão de literatura sobre o atual estado da arte do uso de Blockchain em contextos educacionais (MORAIS; LINS, 2020b). Por fim, com o intuito de manter a propriedade intelectual sobre a solução BlockMoodle, realizou-se o registro do código fonte do software, junto ao Instituto Nacional de Propriedade Intelectual (INPI) (MORAIS; LINS, 2020a).

## 7.3 Trabalhos futuros

O uso de Blockchain na educação é ainda considerado recente, por isso existem alguns desafios relevantes quanto ao uso dessa tecnologia em contextos educacionais. Com base na abordagem proposta neste trabalho são sugeridos alguns trabalhos futuros, que podem ser desenvolvidos para complemento deste e também para utilização em outras aplicações.

Como trabalhos futuros é possível a realização de mais alguns testes de performance da solução proposta, avaliando outras métricas como consumo de memória e CPU, uso de rede, dentre outras coisas. Com isso será possível verificar a existência de possíveis gargalos no sistema, entender porquê o tempo de resposta aumenta consideravelmente para valores superiores a 100, avaliar a sua capacidade de resposta, robustez, disponibilidade, confiabilidade e escalabilidade.

Também é possível a realização de testes de usabilidade na BlockMoodle, para avaliar se a experiência do usuário com a ferramenta é satisfatória. Esta avaliação permitirá

analisar se as funcionalidades e o design aplicado estão próximos ao comportamento de navegação do seu público alvo, que são os profissionais que atuam na área da educação.

A avaliação de custos poderá ser realizada novamente, utilizando dados reais de uma instituição de ensino que realize a oferta de cursos na modalidade EAD, com isso seria possível mensurar qual o gasto necessário para o uso da solução.

É desejável, ainda, a realização de testes de invasão para verificar o nível de segurança apresentado pela solução. Os testes de invasão ou penetração têm como objetivo descobrir e explorar a existência de falhas de segurança, permitindo assim a realização de correções de pontos de vulnerabilidade.





## Referências

- AMATI, F. *First official career diplomas on Bitcoin's Blockchain*. 2015. Disponível em: <<https://blog.signatura.co/first-official-career-diplomas-on-bitcoin-s-blockchain-69311acb544d>>. Acesso em: 21.07.2020. Citado na página 43.
- ANDROULAKI, E. et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: *Proceedings of the thirteenth EuroSys conference*. [S.l.: s.n.], 2018. p. 1–15. Citado na página 42.
- ARENAS, R.; FERNANDEZ, P. CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. *2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018 - Proceedings*, IEEE, p. 1–6, 2018. Citado na página 41.
- ARRUDA, E. P.; ARRUDA, D. E. P. Educação à distância no brasil: políticas públicas e democratização do acesso ao ensino superior. *Educação em Revista*, SciELO Brasil, v. 31, n. 3, p. 321–338, 2015. Citado na página 25.
- BAI, Y. et al. Researchchain: Union Blockchain Based Scientific Research Project Management System. *Proceedings 2018 Chinese Automation Congress, CAC 2018*, IEEE, p. 4206–4209, 2019. Citado na página 44.
- BOESER, B. *Meet truerec by sap: Trusted digital credentials powered by blockchain*. 2017. Disponível em: <<https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain>>. Acesso em: 18.12.2020. Citado na página 40.
- BORE, N. et al. Towards Blockchain-enabled school information hub. *ACM International Conference Proceeding Series*, Part F1320, 2017. Citado na página 42.
- BROILO, L.; NETO, G. B. Pandemia 2020 e a ead: o impacto do covid-19 no ensino brasileiro. *Educação, Cultura e Comunicação*, v. 12, n. 23, 2021. Citado na página 25.
- CHENG, J. C. et al. Blockchain and smart contract for digital certificate. *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*, IEEE, p. 1046–1051, 2018. Citado na página 44.
- CHICARINO, V. et al. Uso de blockchain para privacidade e segurança em internet das coisas. *Livro de Minicursos do VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. Brasília: SBC, p. 28, 2017. Citado 4 vezes nas páginas 25, 31, 32 e 33.
- COELHO, F. C.; BRANDÃO, A. Decentralising scientific publishing: can the blockchain improve science communication? *Memórias do Instituto Oswaldo Cruz*, v. 114, n. July, p. 1–4, 2019. ISSN 0074-0276. Citado na página 48.
- DUAN, B.; ZHONG, Y.; LIU, D. Education application of blockchain technology: Learning outcome and meta-diploma. *Proceedings of the International Conference on*

- Parallel and Distributed Systems - ICPADS*, v. 2017-Decem, p. 814–817, 2018. ISSN 15219097. Citado na página 43.
- GALLARDO, I.; BAZAN, P.; VENOSA, P. Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n. 32, p. 49–66, 2019. Citado na página 39.
- GENCER, A. E. et al. Decentralization in bitcoin and ethereum networks. In: SPRINGER. *International Conference on Financial Cryptography and Data Security*. [S.l.], 2018. p. 439–457. Citado na página 34.
- GIL, A. C. *Métodos e Técnicas de Pesquisa Social*. 6<sup>a</sup>. ed. São Paulo: Atlas, 2008. 8 p. ISBN 978-85-224-5142-5. Citado na página 29.
- GILDA, S.; MEHROTRA, M. Blockchain for Student Data Privacy and Consent. *2018 International Conference on Computer Communication and Informatics, ICCCI 2018*, IEEE, p. 1–5, 2018. Citado na página 45.
- GRECH, A.; CAMILLERI, A. F. *Blockchain in Education - European Commission*. [s.n.], 2017. ISBN 9789279734977. Disponível em: <<https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-education>>. Citado na página 39.
- GULO, C. J. Segurança da informação. jan 2012. Disponível em: <[https://www.researchgate.net/publication/265785308\\_SEGURANCA\\_DA\\_INFORMACAO](https://www.researchgate.net/publication/265785308_SEGURANCA_DA_INFORMACAO)>. Acesso em: 22.11.2018. Citado na página 35.
- HAN, M. et al. A novel blockchain-based education records verification solution. In: *Proceedings of the 19th Annual SIG Conference on Information Technology Education*. [S.l.: s.n.], 2018. p. 178–183. Citado 2 vezes nas páginas 26 e 47.
- HARTHY, K. A.; SHUHAIMI, F. A.; ISMAILY, K. K. J. A. The upcoming blockchain adoption in higher-education: requirements and process. In: IEEE. *2019 4th MEC international conference on big data and smart city (ICBDSC)*. [S.l.], 2019. p. 1–5. Citado 2 vezes nas páginas 26 e 39.
- HOLBL, M. et al. EduCTX: An Ecosystem for Managing Digital Micro-Credentials. *2018 28th EAEEIE Annual Conference, EAEEIE 2018*, IEEE, p. 1–9, 2018. Citado na página 42.
- HUYNH, T. T. et al. Issuing and Verifying Digital Certificates with Blockchain. *International Conference on Advanced Technologies for Communications*, IEEE, v. 2018-Octob, p. 332–336, 2018. ISSN 21621020. Citado na página 40.
- JAIN, R. *The art of computer systems performance analysis*. [S.l.]: john wiley & sons, 2008. Citado na página 66.
- KANAN, T.; OBAIDAT, A. T.; AL-LAHHAM, M. SmartCert BlockChain Imperative for Educational Certificates. *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 - Proceedings*, IEEE, p. 629–633, 2019. Citado na página 41.

- KOLVENBACH, S.; RULAND, R.; GRÄTHER, W. Blockchain 4 Education. *European Conference on Computer-Supported Cooperative Work*, v. 10, n. 5, p. 667–671, 2018. ISSN 00363634. Citado na página 40.
- LIU, Q. et al. Education-industry cooperative system based on blockchain. In: IEEE. *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. [S.l.], 2018. p. 207–211. Citado 3 vezes nas páginas 15, 26 e 46.
- MENASCE, D. A. et al. *Performance by design: computer capacity planning by example*. [S.l.]: Prentice Hall Professional, 2004. Citado na página 66.
- MIKROYANNIDIS, A. et al. Smart Blockchain Badges for Data Science Education. *Proceedings - Frontiers in Education Conference, FIE*, IEEE, v. 2018-Octob, p. 1–5, 2019. ISSN 15394565. Citado na página 43.
- MILLER, R. B. Response time in man-computer conversational transactions. In: *Proceedings of the December 9-11, 1968, fall joint computer conference, part I*. [S.l.: s.n.], 1968. p. 267–277. Citado na página 67.
- MIT, I. *Digital certificates project*. 2016. Disponível em: <<http://certificates.media.mit.edu/>>. Acesso em: 18.12.2020. Citado na página 40.
- MORAIS, A. M. de; LINS, F. A. A. *BlockMoodle*. 2020. BR Patent BR512020002480-7. Disponível em: <<https://gru.inpi.gov.br/pePI/jsp/programas/ProgramaSearchBasico.jsp>>. Citado 2 vezes nas páginas 30 e 70.
- MORAIS, A. M. de; LINS, F. A. A. Uso de blockchain na educação: Estado da arte e desafios em aberto. *Revista Científica Multidisciplinar Núcleo do Conhecimento*, v. 22, p. 78–100, 2020. Citado 3 vezes nas páginas 26, 30 e 70.
- NAKAMOTO, S. A peer-to-peer electronic cash system. *Bitcoin*.–URL: <https://bitcoin.org/bitcoin.pdf>, v. 4, 2008. Citado 3 vezes nas páginas 25, 31 e 33.
- NGUYEN, Q. K.; DANG, Q. V. Blockchain technology for the advancement of the future. In: IEEE. *2018 4th international conference on green technology and sustainable development (GTSD)*. [S.l.], 2018. p. 483–486. Citado na página 25.
- OCHEJA, P.; FLANAGAN, B.; OGATA, H. Connecting decentralized learning records: a blockchain based learning analytics platform. In: *Proceedings of the 8th international conference on learning analytics and knowledge*. [S.l.: s.n.], 2018. p. 265–269. Citado na página 44.
- PAULA, M. T. D. de et al. Desafios na implementação de cursos a distância no ensino superior. In: *I CONEFEA-Tecnologia, Pesquisa e Desafios na Educação Brasileira*. [S.l.: s.n.], 2018. Citado na página 39.
- PLATA, U. N. D. L. 2020. Disponível em: <<https://unlp.edu.ar/>>. Acesso em: 11.04.2020. Citado na página 43.
- PRESSMAN, R. S. *Engenharia de software: uma abordagem profissional*. 6th. ed. Porto Alegre: Bookman, 2009. Citado na página 51.

- PROVDANOV, C. C.; FREITAS, E. C. D. *METODOLOGIA DO TRABALHO CINETÍFICO: Métodos e Técnicas de Pesquisa e do Trabalho Acadêmico*. [S.l.: s.n.], 2013. 128 p. ISSN 1098-6596. ISBN 9788577171583. Citado na página 29.
- RÊGO, B. B. do; GARRIDO, F. A.; MATOS, E. D. S. Moodle como ambiente mooc: orientações para o redesign de interação. *Renote*, v. 16, n. 1, 2018. Citado na página 36.
- ROOKSBY, J.; DIMITROV, K. Trustless Education? A Blockchain System for University Grades. *New Value Transactions Understanding and Designing for Distributed Autonomous Organisations Workshop at DIS 2017*, n. June 2017, p. 4, 2017. Disponível em: <[http://johnrooksby.org/papers/DAOworkshop{\\\_}rooksby](http://johnrooksby.org/papers/DAOworkshop{\_}rooksby)>. Citado na página 45.
- SABBATINI, R. M. Ambiente de ensino e aprendizagem via internet: a plataforma moodle. *Instituto EduMed*, v. 7, 2007. Citado 2 vezes nas páginas 26 e 36.
- SALOMAA, A. Public-key cryptography. Springer Science & Business Media, 2013. Citado na página 32.
- SHARPLES, M.; DOMINGUE, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, v. 9891 LNCS, n. November, p. 490–496, 2016. ISSN 16113349. Citado na página 46.
- SOMMERVILLE, I. *Engenharia de software*. 8th. ed. São Paulo: Pearson, 2007. Citado na página 52.
- SRIVASTAVA, A. et al. A Distributed Credit Transfer Educational Framework based on Blockchain. *Proceedings - 2018 2nd International Conference on Advances in Computing, Control and Communication Technology, IAC3T 2018*, IEEE, p. 54–59, 2019. Citado na página 41.
- STALLINGS, W. *Criptografia e Segurança de Redes, princípios e práticas*. 6<sup>a</sup>. ed. São Paulo: Pearson, 2015. 7 p. ISBN 978-85-430-1450-0. Citado na página 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.
- TEAM, E. *Etherscan: The ethereum block explorer*. 2017. Disponível em: <<https://etherscan.io>>. Acesso em: 06.10.2020. Citado 2 vezes nas páginas 63 e 64.
- 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](https://www.researchgate.net/publication/327161498_Blockchain_Dos_Conceitos_as_Possiveis_Aplicacoes)>. Acesso em: 22.11.2018. Citado na página 34.
- TURKANOVIĆ, M. et al. EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, v. 6, p. 5112–5127, 2018. ISSN 21693536. Citado na página 42.
- WATTERS, A. The Blockchain for Education: An Introduction. *Hack Education*, p. 1–12, 2016. Disponível em: <<http://hackededucation.com/2016/04/07/blockchain-education-guide>>. Citado na página 32.

WOOD, G. et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, v. 151, n. 2014, p. 1–32, 2014. Citado na página 63.

YADAV, R.; SOUSA, E.; CALLOU, G. Performance comparison between virtual machines and docker containers. *IEEE Latin America Transactions*, IEEE, v. 16, n. 8, p. 2282–2288, 2018. Citado na página 66.

ZHONG, J. et al. A Blockchain Model for Word-Learning Systems. *Proceedings - 2018 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing, BESEC 2018*, IEEE, p. 130–131, 2019. Citado 2 vezes nas páginas 26 e 47.