UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE QUIXADÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

MESTRADO ACADÊMICO EM COMPUTAÇÃO

ANTONIO WELLIGTON DOS SANTOS ABREU

UMA ABORDAGEM BASEADA EM BLOCKCHAIN PARA ARMAZENAMENTO E CONTROLE DE ACESSO AOS DADOS DE CERTIFICADOS DE ALUNOS DO ENSINO SUPERIOR

QUIXADÁ

2020

ANTONIO WELLIGTON DOS SANTOS ABREU

UMA ABORDAGEM BASEADA EM BLOCKCHAIN PARA ARMAZENAMENTO E CONTROLE DE ACESSO AOS DADOS DE CERTIFICADOS DE ALUNOS DO ENSINO SUPERIOR

Dissertação apresentada ao Curso de Mestrado Acadêmico em Computação do Programa de Pós-Graduação em Computação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em computação. Área de Concentração: Ciência da Computação

Orientador: Prof. Dr. Emanuel Ferreira Coutinho

QUIXADÁ

2020

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A145a Abreu, Antonio Welligton dos Santos.
Uma Abordagem baseada em blockchain para armazenamento e controle de acesso aos dados de certificados de alunos do ensino superior / Antonio Welligton dos Santos Abreu. – 2020.
146 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Campus de Quixadá, Programa de Pós-Graduação em Computação, Quixadá, 2020.
Orientação: Prof. Dr. Emanuel Ferreira Coutinho.

1. Blockchain (Base de dados). 2. Contrato inteligente. 3. Certificados. 4. Ensino superior. I. Título.
CDD 005

ANTONIO WELLIGTON DOS SANTOS ABREU

UMA ABORDAGEM BASEADA EM BLOCKCHAIN PARA ARMAZENAMENTO E CONTROLE DE ACESSO AOS DADOS DE CERTIFICADOS DE ALUNOS DO ENSINO SUPERIOR

Dissertação apresentada ao Curso de Mestrado Acadêmico em Computação do Programa de Pós-Graduação em Computação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em computação. Área de Concentração: Ciência da Computação

Aprovada em: ____/_____/_____.

BANCA EXAMINADORA

Prof. Dr. Emanuel Ferreira Coutinho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Regis Pires Magalhães
Universidade Federal do Ceará (UFC)

Prof. Dr. Gabriel Antoine Louis Paillard
Universidade Federal do Ceará (UFC)

Prof. Dr. Valdemar Vicente Graciano Neto
Universidade Federal de Goiás (UFG)

Dedico a minha família, em especial minha mãe Aurea. Ela sempre me ensinou a lutar por meus objetivos de forma honesta e com respeito ao próximo.

AGRADECIMENTOS

Primeiramente a Deus, pois ele sempre me guiou pelos melhores caminhos da vida e sem ele esse trabalho não poderia ser realizado.

Ao meu orientador, Emanuel Coutinho, por me apoiar durante todas as etapas desse trabalho. Serei grato eternamente por todos seus ensinamentos e companheirismo para enfrentar e superar todas as dificuldades que surgiram durante esse trabalho. Muito obrigado!

Agradeço a minha esposa Kelly Cássia pelo companheirismo e apoio ao longo dessa jornada difícil, pois por diversos momentos fiquei ausente para se dedicar exclusivamente a esse trabalho.

Agradeço aos meus sogros Rita e Stênio por me apoiar durante momentos cruciais durante esse trabalho. A presença e atenção de vocês foram muito importante para o alcance dessa vitória.

A minha família que sempre está disposta a fazer o impossível para me ajudar durante as batalhas da vida. Eles me deram todo o apoio e incentivo necessário para eu conseguir sair vitorioso nessa jornada.

Por fim, agradeço a todos que participaram da validação da aplicação desenvolvida nesse trabalho.

“A grandeza não consiste em receber honras, mas em merecê-las.”

(Aristóteles)

RESUMO

Blockchain é considerada uma tecnologia emergente, tendo despertado o interesse de pesquisadores e indústrias no cenário mundial. Após o sucesso dessa tecnologia no mercado financeiro com as moedas virtuais (Bitcoin e Litecoin), a *blockchain* começa a ser utilizada por diferentes domínios, como governo e educação, pois proporciona um ambiente distribuído confiável, escalável e imutável para a realização e armazenamento de transações em uma rede. Contratos inteligentes são um dos recursos da *blockchain* Ethereum, que possui a capacidade de executar um modelo de programação para aplicações distribuídas em ambientes não confiáveis. Esses contratos residem na *blockchain* e possibilitam a automação de processos em várias etapas. Os contratos inteligentes se tornaram uma das tecnologias mais procuradas devido à alta customização que adicionam às transações, permitindo buscar soluções baseadas em *blockchain* para problemas na indústria e academia. O ensino superior é um sistema com vários desafios que podem ser resolvidos com adoção dessa tecnologia. Proteger as transações de dados que envolvem diplomas de estudantes é um dos desafios considerados pelas instituições de ensino. Dessa forma, neste trabalho é apresentada uma proposta de arquitetura que tem como base a tecnologia *blockchain* para armazenar e consultar dados de diplomas emitidos por instituições de ensino superior. Por meio dessa arquitetura, foi avaliada uma nova abordagem para a validação dos dados de diplomas com essa tecnologia emergente. Como prova de conceito, foi implementado um protótipo do ambiente utilizando contratos inteligentes baseado na plataforma Ethereum. Após implementação foi realizada uma avaliação com especialistas na gestão de diplomas e realizada uma análise de desempenho das transações realizadas no protótipo. Diante dos resultados obtidos, a proposta se mostrou adequada ao processo de armazenar e consultar dados de diplomas.

Palavras-chave: Blockchain. Contratos Inteligentes. Gerenciamento de Certificados. Ensino Superior.

ABSTRACT

Blockchain is considered an emerging technology, having aroused the interest of researchers and industries on the world stage. After the success of this technology in the financial market with virtual currencies (such as Bitcoin and Litecoin), blockchain starts to be used by different domains, such as government and education, as it provides a reliable, scalable and immutable distributed environment for the realization and storage of transactions on a network. Smart contracts are one of the features of the Ethereum blockchain, which has the ability to run a programming model for applications distributed in untrusted environments. These contracts reside on the blockchain and enable process automation in several stages. Smart contracts have become one of the most sought-after technologies due to the high customization they add to transactions, allowing to seek blockchain-based solutions to problems in industry and academia. Higher education is a system with several challenges that can be solved with the adoption of this technology. Protecting data transactions involving student degrees is one of the challenges considered by educational institutions. Thus, this work presents an architecture proposal based on blockchain technology to store and consult data from diplomas issued by higher education institutions. Through this architecture, a new approach for the validation of diploma data with this emerging technology was evaluated. As a proof of concept, a prototype of the environment was implemented using smart contracts based on the Ethereum platform. After implementation, an evaluation was carried out with specialists in the management of diplomas and an analysis of the performance of the transactions carried out in the prototype was carried out. In view of the results obtained, the proposal proved to be adequate to the process of storing and consulting diploma data.

Keywords: Blockchain. Smart Contracts. Certificate Management. Higher Education.

LISTA DE FIGURAS

Figura 1 – Fluxo das atividades que foram realizadas 22
Figura 2 – Exemplo de publicação no Diário Oficial da União (DOU) 27
Figura 3 – Exemplo de *blockchain* e seus blocos 30
Figura 4 – Transações com *hash* em uma Árvore Merkle 35
Figura 5 – Os estados anteriores estão ligados ao estado atual 35
Figura 6 – Esquema de sistema de criptomoeda com contratos inteligentes 43
Figura 7 – *Blockchain* como um componente em uma arquitetura de software 51
Figura 8 – *Blockchain* como um componente de sistemas de aplicativos de software . . 51
Figura 9 – Arquitetura de referência de plataformas de *blockchain* 52
Figura 10 – Visão geral do caminho de decisão da *blockchain* 55
Figura 11 – Quantidade de trabalhos por ano 58
Figura 12 – Quantidade de trabalhos por país 59
Figura 13 – Nuvem de palavras construída pelas palavras chave dos trabalhos 59
Figura 14 – Arquitetura de referência de *blockchain* proposta 70
Figura 15 – Arquitetura proposta 72
Figura 16 – Visão geral do fluxo da aplicação proposta 74
Figura 17 – Visão ampliada da arquitetura proposta 78
Figura 18 – Fluxo de execução das tecnologias utilizadas 82
Figura 19 – Operação de implantação do contrato inteligente na IDE Remix com integração com plugin MetaMask 84
Figura 20 – Página principal da aplicação Educ-Dapp 85
Figura 21 – Página de *login* da aplicação Educ-Dapp 86
Figura 22 – Página da aplicação para cadastrar IES regular 87
Figura 23 – Página de autocadastro da IES 87
Figura 24 – Página de cadastro de diploma 88
Figura 25 – Página de revogação de diploma 88
Figura 26 – Página de consulta e resultado da busca por diploma na *blockchain* 89
Figura 27 – Cadastro de IES regular com confirmação do MetaMask 90
Figura 28 – Autocadastro da IES com confirmação do MetaMask 91
Figura 29 – Cadastro de diploma realizado pela IES 91
Figura 30 – Questões demográficas sobre experiência profissional e em certificados . . . 94

Figura 31 – Detalhes de um bloco criado na blockchain 98
Figura 32 – Histograma e *boxplot* para valores coletados de *ether* da funcionalidade de cadastro de diplomas 101
Figura 33 – Histograma e *boxplot* para valores coletados de *gas* da funcionalidade de cadastro de diplomas 101
Figura 34 – Histograma e *boxplot* para valores coletados do tempo (segundos) para minerar o bloco da funcionalidade de cadastro de diplomas 102
Figura 35 – Histograma e *boxplot* para valores coletados de *ether* da funcionalidade de revogação de diplomas 104
Figura 36 – Histograma e *boxplot* para valores coletados de *gas* da funcionalidade de revogação de diplomas 104
Figura 37 – Histograma e *boxplot* para valores coletados do tempo (segundos) para minerar o bloco da funcionalidade de revogação de diplomas 105
Figura 38 – Histograma e *boxplot* para valores coletados de *ether* da funcionalidade de atualização de diplomas 107
Figura 39 – Histograma e *boxplot* para valores coletados de *gas* da funcionalidade de atualização de diplomas 107
Figura 40 – Histograma e *boxplot* para valores coletados do tempo (segundos) para minerar o bloco da funcionalidade de atualização de diplomas 108
Figura 41 – Histograma e *boxplot* para valores coletados do tempo (segundos) para minerar o bloco da funcionalidade de consulta de diplomas 110
Figura 42 – Passo inicial instalação MetaMask. 127
Figura 43 – Criar uma conta no MetaMask. 128
Figura 44 – Termos da conta do MetaMask. 128
Figura 45 – Informar senha e aceitar os termos do MetaMask. 128
Figura 46 – Acesso as palavras chaves da conta MetaMask. 129
Figura 47 – Visualizar as palavras chaves da conta MetaMask. 129
Figura 48 – Confirmar as palavras chaves da conta MetaMask. 129
Figura 49 – Confirmação que a conta foi criada com sucesso. 130
Figura 50 – Tela inicial do MetaMask. 130
Figura 51 – Selecionar rede de testes da Ethereum. 131
Figura 52 – Requisitar 1 Ether falso. 131

Figura 53 – Seguir para confirmação da transferência de 1 Ether. 132
Figura 54 – Confirmação para transferência de 1 Ether. 132
Figura 55 – *Hash* da transferência de 1 Ether do site opção 1 132
Figura 56 – Copiar endereço da conta MetaMask. 133
Figura 57 – Campo para informar endereço da conta MetaMask. 133
Figura 58 – *Hash* da transferência de 1 Ether do site opção 2. 134
Figura 59 – Valor de 1 Ether na conta do MetaMask. 134
Figura 60 – Página principal da aplicação Educ-Dapp. 135
Figura 61 – Média de Gwei. 136
Figura 62 – Acessar área de login da aplicação. 137
Figura 63 – Seguir para confirmação do MetaMask para interagir com aplicação. 137
Figura 64 – Confirmação do MetaMask para interagir com aplicação. 138
Figura 65 – Acessar tela de login da aplicação. 138
Figura 66 – Login do governo na aplicação. 139
Figura 67 – Página da aplicação para cadastrar IES regular. 139
Figura 68 – Cadastro de IES regular com confirmação do MetaMask. 140
Figura 69 – Página de autocadastro da IES. 140
Figura 70 – Autocadastro da IES com confirmação do MetaMask. 141
Figura 71 – Login da IES na aplicação. 141
Figura 72 – Seleção de função cadastrar diplomas. 142
Figura 73 – Cadastro de diploma. 143
Figura 74 – Cadastro de diploma realizado pela IES. 144
Figura 75 – Acesso a consulta de diplomas. 144
Figura 76 – Mensagem de validação com sucesso. 145
Figura 77 – Consulta e resultado da busca por diploma na blockchain. 145
Figura 78 – Seleção de função revogar diploma 145
Figura 79 – Revogação de diploma. 146
Figura 80 – Confirmação do MetaMask para Revogar de diploma. 146
Figura 81 – Mensagem de diploma não registrado. 146

LISTA DE TABELAS

Tabela 1 – Comparação entre trabalhos relacionados (I = incluir, V = validar, C = consultar, R = revogar) 63
Tabela 2 – Comparação entre trabalhos relacionados 64
Tabela 3 – Questões demográficas (QD), sobre a aplicação (QA) e de opinião (QO) do questionário 92
Tabela 4 – Critérios para avaliação de desempenho para os experimentos 99
Tabela 5 – Valores estatísticos para a funcionalidade de cadastro de diploma 103
Tabela 6 – Valores estatísticos para a funcionalidade de revogação de diploma 105
Tabela 7 – Valores estatísticos para a funcionalidade de atualização de diploma 108
Tabela 8 – Valores estatísticos para a funcionalidade de consulta de diploma 110

LISTA DE QUADROS

Quadro 1 – Lista de veículos de publicação identificados na pesquisa 60
Quadro 2 – Artigos publicados em conferências e periódicos 116

LISTA DE ABREVIATURAS E SIGLAS

DOU	Diário Oficial da União
IES	Instituição de Ensino Superior
TI	Tecnologia da Informação
IoT	*Internet of Things*
MEC	Ministério da Educação do Brasil
P2P	*Peer-to-Peer*
PoW	*Proof-of-Work*
PoS	*Proof-of-Stake*
BFT	*Byzantine Fault Tolerance*
IP	*Internet Protocol*
DApp	*Decentralized Application*
EVM	*Ethereum Virtual Machine*
DoS	*Denial Of Service*
API	*Application Programming Interface*
MV	Máquina Virtual
RF	Requisitos Funcionais
RNF	Requisitos Não Funcionais
ABI	*Application Binary Interface*
TCLE	Termo de Consentimento Livre e Esclarecido

SUMÁRIO

1 INTRODUÇÃO 18
1.1 Motivação 18
1.2 Objetivos 21
1.3 Metodologia 22
1.4 Contribuições 24
1.5 Organização do Trabalho 25
2 FUNDAMENTAÇÃO TEÓRICA 26
2.1 Diplomas 26
2.1.1 Registro de Diplomas no Ensino Superior 26
2.1.2 Acesso aos Diplomas no Ensino Superior 27
2.2 *Blockchain* 28
2.2.1 Surgimento e Definição de Blockchain 29
2.2.2 Estrutura da Blockchain 31
2.2.2.1 Rede Peer-to-Peer *31*
2.2.2.2 Criptografia *32*
2.2.2.3 Árvore de Merkle *34*
2.2.3 Consenso 35
2.2.3.1 Problema do Gasto Duplo *36*
2.2.3.2 Algoritmo Proof-of-Work *37*
2.2.3.3 Algoritmo Proof-of-Stake *38*
2.2.4 Tipos de Blockchain e Plataformas 39
2.3 Contratos Inteligentes 42
2.4 Ethereum 45
2.4.1 Conceitos Elementares 47
2.4.1.1 Gas e Ether *47*
2.4.1.2 Transações *48*
2.4.2 Mineração 49
2.5 Arquiteturas para *Blockchain* 50
2.6 Principais Aplicações da *Blockchain* 53
2.7 Analisando Adoção da Tecnologia *Blockchain* 55

3 TRABALHOS RELACIONADOS 57
3.1 Planejamento da Busca por Trabalhos Relacionados 57
3.2 Visão Geral 58
3.3 Descrição dos Trabalhos Relacionados e Comparação 59
4 ARQUITETURA E APLICAÇÃO EDUC-DAPP 65
4.1 Análises Preliminares 65
4.1.1 Protótipo 65
4.1.2 Etapas para Avaliação da Blockchain 66
4.1.3 Avaliação de Uso Comparada ao Processo Atual 67
4.2 Arquitetura 68
4.3 Requisitos da Aplicação 76
4.4 Modelagem da Aplicação 77
5 DESENVOLVIMENTO E AVALIAÇÃO DE DESEMPENHO DO PROTÓTIPO DA ARQUITETURA PROPOSTA UTILIZANDO CONTRATOS INTELIGENTES 80
5.1 Implementação da Solução Proposta 80
5.1.1 Infraestrutura 80
5.1.2 Contratos Inteligentes 82
5.1.3 Aplicação Web 85
5.2 Cenário de Avaliação 89
5.2.1 Projeto 91
5.2.2 Avaliação com Usuários 93
5.3 Avaliação de Desempenho 97
5.3.1 Projeto do Experimento 97
5.3.2 Execução 99
5.3.3 Cadastro de Diplomas e Instituições 100
5.3.4 Revogação de Diplomas 103
5.3.5 Atualização de Diplomas 106
5.3.6 Consulta de Diplomas 109
5.4 Análises e Discussão 110
6 CONCLUSÃO 114
6.1 Considerações Finais 114

6.2 Publicações 116
6.3 Limitações do Trabalho 117
6.4 Trabalhos Futuros 118
REFERÊNCIAS 120
APÊNDICE A–MANUAL DE INSTALAÇÃO DO METAMASK 127
A.1 Detalhes da Instalação 127
A.2 Conseguir Criptomoeda para Testes 130
APÊNDICE B–MANUAL DE UTILIZAÇÃO DA EDUC-DAPP 135
B.1 Cadastrar IES 136
B.2 Cadastrar Diploma 142
B.3 Consultar Diploma 142
B.4 Revogar Diploma 143

1 INTRODUÇÃO

Com o avanço da tecnologia nos últimos anos nas mais diversas áreas, cresceu a necessidade da proteção dos dados das pessoas e instituições inseridas no meio acadêmico e industrial. Os alunos graduados de uma Instituição de Ensino Superior (IES) podem necessitar de uma comprovação, por meio dos certificados, caso participem de algum processo de seleção. No entanto, muitas vezes acabam perdendo os certificados impressos, sendo necessário solicitar uma cópia na instituição responsável pela emissão desse documento, que pode levar um determinado tempo por causa dos processos administrativos para validação dos dados para emissão do certificado. Por outro lado, solicitar uma cópia eletrônica pode economizar papel, tempo e recursos financeiros (CHENG *et al.*, 2018).

Os graduados podem solicitar facilmente qualquer certificado ao fornecer as informações que verifiquem sua identidade. No entanto, por causa dessa conveniência, a probabilidade de falsificação dos certificados é alta. Com isso, instituições educacionais e empresas não podem validar rapidamente os documentos que recebem (CHENG *et al.*, 2018).

1.1 Motivação

A maioria das instituições de ensino superior possuem seu próprio sistema especializado para manter os registros completos dos cursos e alunos, em que os dados estão estruturados para serem acessados somente pela equipe determinada da instituição ou pelos alunos de maneira restrita em sites ou sistemas dedicados para esse fim, tendo pouca ou nenhuma interoperabilidade. Em geral, os bancos de dados desses sistemas estão hospedados em um *datacenter* dentro das IES, com acesso restrito aos seus profissionais de Tecnologia da Informação (TI) (TURKANOVIć *et al.*, 2018). Nas IES, a emissão e disponibilidade do certificado estão desempenhando um papel crítico, pois ele é uma forte evidência que o aluno concluiu o curso com sucesso (HARTHY *et al.*, 2019). Com isso, é importante a prevenção de fraudes de transcrição do diploma assim como um local na *web* para verificar a veracidade dos dados emitidos pela instituição.

Diante deste cenário, pode-se observar alguns desafios no controle de acesso e segurança dos dados dos diplomas dos alunos: (i) o fato de haver várias bases de dados diferentes com suas próprias restrições de acesso e mecanismos de segurança podem se tornar um fator de complicação no gerenciamento das informações emitidas pelas IES em território regional ou nacional; (ii) a necessidade de não ter terceiros envolvidos no processo de validação dos

dados de um diploma também é um desafio, pois os alunos acabam necessitando da IES que emitiu o certificado para comprovar sua formação diante de uma seleção de vaga de emprego ou continuação dos estudos; (iii) o fato de não depender de um processo administrativo manual ou da disponibilidade de um sistema da IES para comprovar um diploma pode ser uma situação de melhoria a ser considerada; (iv) cada IES é responsável pelo armazenamento seguro dos dados dos diplomas dos alunos, em que isso pode ser um fator preocupante, pois os mecanismos utilizados por cada uma podem não ser os mais adequados para armazenar de forma segura os dados por um longo período de tempo, causando a perda das informações; e (v) impedir documentos falsificados é um dos grandes desafios do ensino superior, sendo necessário ter algum mecanismo de verificabilidade dos dados para evitar a falsificação de certificados.

Todos esses problemas mencionados podem ser tratados com tecnologias tradicionais, podendo ser sistemas centralizados ou descentralizados. Nos sistemas descentralizados temos, por exemplo, os diferentes padrões de arquiteturas e os protocolos de comunicação dos mecanismos convencionais de sistemas distribuídos (*CORBA, .net, RMI, SOAP, REST*). Em sistemas distribuídos temos diversos componentes distribuídos por diferentes servidores, que podem ser heterogêneos, com diferentes sistemas operacionais, fabricantes e capacidades de processamento. Em sistemas centralizados isso não existe, pois há um único componente que é o próprio sistema centralizado, tendo como principal desvantagem problemas relacionados a disponibilidade e centralização dos dados (IVAKI *et al.*, 2018). Mesmo com uma grande variedade de mecanismos nessas tecnologias convencionais para tratar a segurança dos dados, ainda existem alguns desafios como integridade e confiabilidade das transações dos sistemas, no qual essas tecnologias tentam melhorar a cada dia para evitar problemas de segurança dos dados envolvidos nas transações (XU *et al.*, 2019).

Como alternativa tecnológica para tratar os cenários de problemas mencionados, em que é necessário ocorrer transações entre partes confiáveis (IES do aluno, aluno, empresas, pessoas interessadas, governo e outras IES) para validação, armazenamento, disponibilidade e segurança dos dados dos diplomas, existe a tecnologia emergente denominada *blockchain*, que pode tratar de forma mais adequada os problemas mencionados. As soluções criadas através da tecnologia *blockchain* permitem alta confiabilidade, desintermediação e transações verificadas (TAUFIQ *et al.*, 2019).

Blockchain é uma inovação tecnológica introduzida em 2008 com a criptomoeda chamada Bitcoin, sendo um livro de contabilidade ponto a ponto para registrar as transações

(NAKAMOTO, 2008). O objetivo era eliminar qualquer intermediário e permitir que os usuários façam suas transações diretamente. Para conseguir isso, a *blockchain* foi projetada como uma rede descentralizada de nós (ALAMMARY *et al.*, 2019), que geralmente é representada como uma cadeia de blocos, sendo cada bloco uma sequência lógica de transações, que são registros permanentes, transparentes e imutáveis (THAKKAR *et al.*, 2018).

A tecnologia *blockchain* está lentamente se integrando em diferentes domínios, como logística, energia, saúde e identificação digital. Um dos domínios adequados para a adoção da tecnologia *blockchain* é o ensino superior, no qual os princípios da autenticação de documentos, transparência, imutabilidade e confiança são as principais vantagens que tornam essa combinação adequada (GRECH; CAMILLERI, 2017). Além de sua aplicação em criptomoeda, a tecnologia *blockchain* possui aplicações com potencial em outras áreas, como Internet das Coisas (do inglês *Internet of Things* (IoT)) (HUH *et al.*, 2017), gerenciamento da cadeia de suprimentos (KORPELA *et al.*, 2017) e armazenamento de dados médicos (AZARIA *et al.*, 2016).

Muitos dos aspectos inovadores da tecnologia *blockchain* (por exemplo, contratos inteligentes) são relativamente novos (BOSU *et al.*, 2019). Embora o número de projetos de software com *blockchain* tenha crescido nos últimos dois anos, muitas ferramentas e bibliotecas que possam suportar seu desenvolvimento ainda estão em fase de desenvolvimento. Como a *blockchain* é uma tecnologia nova, há escassez de desenvolvedores com domínio suficiente em comparação com a maioria dos domínios não *blockchain*.

As soluções baseadas em *blockchain* aceleram e facilitam procedimentos administrativos em que um processo de validação é necessário. Os certificados concedidos aos alunos para reconhecer os resultados alcançados na realização de um curso em uma IES são os principais documentos que exigem um processo de verificação. A tecnologia *blockchain* permite colocar a credibilidade e controle sobre os certificados dos alunos, eliminando assim a necessidade de um processo de verificação por um intermediário (por exemplo, a IES) (KAMIŠALIĆ *et al.*, 2019).

No Brasil o processo de registro de diploma envolve documentos dos alunos e das IES que são indispensáveis para garantir a segurança e validade dos atos jurídicos a serem produzidos por esse processo, sendo que o registro do diploma deverá ser feito em livro próprio no meio físico ou eletrônico, a critério de cada instituição. Seguindo o ato administrativo da portaria de número 1.095 pelo Ministério da Educação do Brasil (MEC), após o registro é necessário publicar extrato das informações sobre o registro no DOU, pagando um determinado valor financeiro pelo espaço utilizado na publicação, na qual a responsabilidade pela publicação

das informações no DOU é de cada IES expedidora. O objetivo dessa nova lei é dar mais credibilidade e segurança às informações dos diplomas dos alunos (BRASIL, 2018).

1.2 Objetivos

Neste contexto, este trabalho propõe um modelo de arquitetura utilizando a tecnologia *blockchain*, em que essa nova abordagem sugerida trata de ter uma infraestrutura fisicamente distribuída, mas logicamente centralizada, fornecendo uma visão única da veracidade sobre os dados dos diplomas dos alunos para todas as partes interessadas. Com isso, o objetivo geral deste trabalho é fornecer um ambiente com credibilidade e segurança através da tecnologia *blockchain* para publicar extrato das informações de diplomas de alunos do ensino superior, assim como também a consulta para validação dos dados do diploma. Com essa tecnologia é possível diminuir os riscos de perda das informações, além de economizar papel, reduzir custos de gerenciamento e impedir documentos falsificados, pois através do princípio da verificabilidade dos dados pode-se evitar a falsificação de certificados.

Os objetivos específicos são: (i) criar uma infraestrutura que atenda as necessidades da proposta; (ii) propor uma arquitetura de referência; (iii) desenvolver uma aplicação para publicar extrato das informações e validar os dados dos diplomas; (iv) criar um cenário de avaliação; (v) aplicar um questionário a profissionais experientes da área educacional; e (vi) realizar um estudo de análise de desempenho da aplicação criada.

O foco principal da pesquisa é buscar construir uma abordagem que utiliza a tecnologia *blockchain* e identificar respostas às seguintes questões:

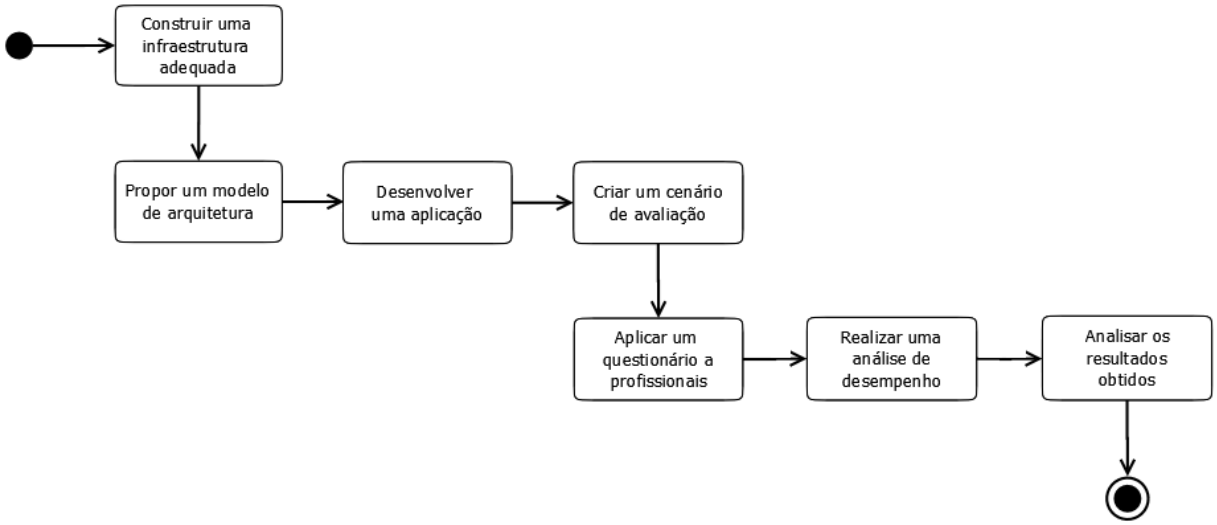
- Questão 1: quais os principais desafios tecnológicos que as instituições educacionais podem enfrentar para inovar na área de gestão dos dados dos diplomas utilizando a tecnologia *blockchain*?
- Questão 2: é possível criar uma solução baseada em *blockchain* para atender os requisitos da portaria de número 1.095 do MEC, que exige a publicação de um extrato das informações sobre os registros realizados no DOU?
- Questão 3: existem diferenças significativas do ponto de vista do usuário final entre uma solução baseada em *blockchain* e uma solução tradicional para manter um banco de informações de registro de diplomas a ser disponibilizado na *web*, após realizado o devido registro dos diplomas no DOU?

1.3 Metodologia

O presente trabalho foi subdividido em algumas etapas com intuito de cumprir os objetivos elencados anteriormente. Inicialmente algumas atividades comuns de pesquisa foram executadas para compreender melhor os conceitos e mecanismos relacionados a tecnologia *blockchain*. Estas atividades foram: um levantamento bibliográfico, um estudo de trabalhos relacionados e uma análise de ferramentas e tecnologias específicas. Todas essas etapas foram com foco para o desenvolvimento de uma solução baseada em *blockchain*.

As demais etapas da pesquisa estão relacionadas em um diagrama de atividades, apresentado na Figura 1 para melhorar o entendimento da execução das atividades.

Figura 1 – Fluxo das atividades que foram realizadas



Fonte: Elaborado pelo autor.

A descrição de cada etapa está detalhada logo a seguir:

- **Construir uma infraestrutura adequada:** Para realizar o estudo deste trabalho foi necessário criar uma infraestrutura que atenda às necessidades da proposta. Essa etapa consistiu em utilizar as ferramentas e tecnologias para construir a estrutura necessária baseada em *blockchain*. A intenção é ter um ambiente que possibilite às entidades (estudante, instituições educacionais, empresas e governo) envolvidas durante o estudo acessarem através da *web* as funcionalidades da aplicação que foi desenvolvida. Todas as funcionalidades tem sua usabilidade semelhante a um sistema tradicional, em que de maneira transparente tem uma *blockchain* interagindo como *back-end* com o *front-end* da aplicação.
- **Propor um modelo de arquitetura**: É necessário ter uma definição de como vai ser o fluxo dos dados entre as entidades envolvidas neste trabalho. Com isso, foi proposto um

modelo de arquitetura para organizar as funcionalidades do ambiente, a interação entre as entidades e o controle de acesso aos dados, na qual essa estrutura serviu como base para o desenvolvimento da aplicação *web*. Também uma das principais decisões de arquitetura que foi tomada é sobre quais dados das entidades deveriam ser colocados na cadeia de blocos.

- **Desenvolver uma aplicação:** Após montar a infraestrutura e definir uma proposta de arquitetura, o desenvolvimento da aplicação foi iniciado. Para isto, a infraestrutura utilizada deverá ser capaz de se comunicar com uma *blockchain* para enviar dados para serem armazenados e depois consultados. O intuito é proporcionar o acesso para as entidades via *Internet* a uma rede *blockchain* através de algumas funcionalidades oferecidas pela aplicação *web*. Essas funcionalidades são específicas para publicar o extrato das informações e validar os dados dos diplomas.
- **Criar um cenário de avaliação:** Uma vez criada a aplicação, o passo seguinte foi definir um cenário de avaliação para ilustrar o funcionamento do ambiente. Foi definido um cenário de utilização para algumas instituições de ensino superior realizarem a avaliação, em que os usuários participantes foram pessoas com experiência no processo de emissão de diplomas. Os dados utilizados durante a avaliação foram fictícios. Porém, os dados inseridos na *blockchain* foram formatados com base na portaria de número 1.095 do MEC, que define as regras no governo brasileiro para o registro de diplomas.
- **Aplicar um questionário a profissionais:** Após a conclusão da avaliação foi aplicado um questionário sobre a solução proposta aos profissionais participantes, buscando investigar justificativas para apoiar decisões arquitetônicas sobre se devem empregar uma *blockchain* ou algum sistema convencional. Também foi avaliado o uso do ambiente criado comparando o mesmo ao processo atual exigido pela portaria de número 1.095 do MEC para publicação de extrato das informações sobre o registro dos diplomas.
- **Realizar uma análise de desempenho:** Esta etapa consistiu em realizar um estudo empírico para analisar o desempenho das transações realizadas no ambiente criado. O objetivo foi identificar possíveis gargalos de desempenho nas transações realizadas, compreendendo melhor o comportamento de sistemas baseados em *blockchain*. Medições foram realizadas durante cada transação para coletar o tempo necessário para seu processamento e os custos de execução. Assim pode-se determinar a média, valores mínimo e máximo, mediana, quartis e desvio padrão de tempo e custos das transações. Também foi analisado o tempo

de consulta aos dados após armazenamento na *blockchain*.

– **Analisar os resultados obtidos:** Por fim, após a execução das etapas anteriores, as informações foram consolidadas para avaliar os resultados obtidos. O intuito é verificar se existem benefícios significativos para gestão dos dados de diplomas utilizando uma solução baseada em *blockchain*. Para isso, gráficos e relatórios com os resultados obtidos para analisar as informações foram projetados e desenvolvidos, em seguida, foram relacionados com os objetivos deste trabalho e as questões de pesquisa definidas.

1.4 Contribuições

Com base na pesquisa bibliográfica realizada e na experiência adquirida no desenvolvimento e aplicação dos conceitos estudados, pode-se listar as seguintes contribuições desse trabalho:

– Definição de uma arquitetura de referência identificando os principais componentes de uma solução *web* baseada em *blockchain* para melhorar a compreensão e facilitar o desenvolvimento de aplicações;
– Definição de uma abordagem baseada em *blockchain* como alternativa para atender o ato administrativo da portaria de número 1.095 do MEC, que define a necessidade de manter um banco de informações de registro de diplomas a ser disponibilizado na *web*, após realizado o devido registro dos diplomas no DOU;
– Desenvolvimento de uma aplicação *web* para demonstrar na prática uma solução que utiliza *blockchain* para armazenar dados de certificados de alunos;
– Levantamento detalhado de um conjunto de ferramentas que proporciona o desenvolvimento de soluções *web* com *blockchain*;
– Avaliação de uma aplicação *web* baseada em *blockchain* por especialistas da área educacional como forma de analisar uma solução para armazenar dados de certificados de alunos;
– Realização de uma análise de desempenho do tempo e custos das transações realizadas em uma aplicação *web* que utiliza *blockchain*, considerando que as coletas foram realizadas durante a avaliação da aplicação por especialistas da área educacional.

1.5 Organização do Trabalho

O restante do documento está dividido nos seguintes capítulos. No Capítulo 2 é apresentada a descrição do domínio de diplomas e os conceitos relacionados a *blockchain* e contratos inteligentes levantados através da pesquisa bibliográfica. No Capítulo 3, alguns trabalhos relacionados são discutidos para melhorar o entendimento do cenário trabalhado. No Capítulo 4 são apresentadas as análises iniciais do trabalho, os detalhes da arquitetura proposta e os requisitos para o desenvolvimento da solução. No Capítulo 5, são apresentadas as etapas realizadas para o desenvolvimento e avaliação da solução criada, bem como as análises e discussão das experiências vivenciadas com a tecnologia *blockchain*. Por fim, o Capítulo 6 apresenta as conclusões desse trabalho, em que descreve também as limitações identificadas e perspectivas de trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo trata da fundamentação teórica utilizada neste trabalho. São abordados os conceitos das áreas de educação (diplomas no ensino superior) e *blockchain* que foram utilizados para alcançar os objetivos deste trabalho.

2.1 Diplomas

De acordo com o MEC, mais de 1 milhão de alunos do ensino superior se formam em todo o Brasil a cada ano, sendo que em 2018 foram cerca 1,2 milhão de estudantes graduados (MEC, 2019). Alguns deles vão para outros países e instituições para continuar os estudos e outros entrarão em um emprego. Os certificados que os alunos recebem após conclusão de um curso comprovam sua formação e desempenho, tornando os mesmos uma referência importante para a entrada em outras instituições ou novos trabalhos (CHENG *et al.*, 2018).

Existem pontos vitais em relação aos sistemas responsáveis pelo controle dos dados educacionais, como padronização de dados, local de armazenamento, segurança e como filtrar, analisar, proteger e compartilhar esses dados. Conectadas a esses problemas, as instituições de ensino superior mantêm o registro dos dados completos dos alunos por período indeterminado por razões legais, dependendo da política de um país (TURKANOVIć *et al.*, 2018).

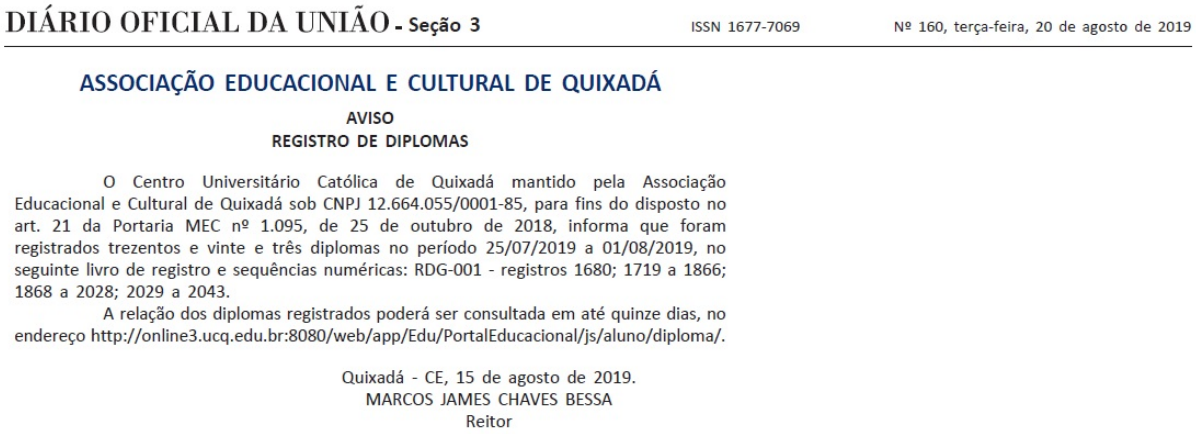
As credenciais acadêmicas são ativos importantes para um indivíduo, pois elas fornecem uma identificação acadêmica de uma pessoa. Certificados falsificados são um problema que as instituições enfrentam diariamente. Algumas empresas estudam uma forma de melhorar os mecanismos de verificação da legitimidade desses documentos (KANAN *et al.*, 2019). O cenário ideal para instituições educacionais é fornecer ao aluno um registro público persistente, protegido contra alterações ou perda de seus registros particulares. A Universidade de Nicosia foi a primeira instituição de ensino superior a emitir certificados acadêmicos cujos autenticidade pode ser verificada através da *blockchain* Bitcoin (SHARPLES; DOMINGUE, 2016).

2.1.1 Registro de Diplomas no Ensino Superior

No Brasil, em 25 de outubro de 2018 foi expedido o ato administrativo da portaria de número 1.095 pelo Ministério da Educação, determinando que as "IES públicas e privadas que possuem prerrogativa para o registro dos diplomas por elas expedidos deverão publicar extrato das informações sobre o registro no DOU" (BRASIL, 2018, p. 7), que representa um

veículo de comunicação pelo qual a Imprensa Nacional do Brasil torna público todo e qualquer assunto acerca do âmbito federal. Na Figura 2 é apresentado um exemplo de publicação oficial de uma IES privada. No extrato das informações publicadas no DOU deverá conter, no mínimo, as seguintes informações: (i) nome da mantenedora e da mantida; (ii) número do CNPJ da mantenedora; (iii) quantidade de diplomas registrados no período; (iv) intervalo dos números de registro dos diplomas; (v) identificação do número do livro de registro; e (vi) identificação do sítio eletrônico da IES no qual poderá ser consultada a relação de diplomas registrados.

Figura 2 – Exemplo de publicação no DOU



DIÁRIO OFICIAL DA UNIÃO - Seção 3 ISSN 1677-7069 Nº 160, terça-feira, 20 de agosto de 2019

ASSOCIAÇÃO EDUCACIONAL E CULTURAL DE QUIXADÁ

AVISO
REGISTRO DE DIPLOMAS

O Centro Universitário Católica de Quixadá mantido pela Associação Educacional e Cultural de Quixadá sob CNPJ 12.664.055/0001-85, para fins do disposto no art. 21 da Portaria MEC nº 1.095, de 25 de outubro de 2018, informa que foram registrados trezentos e vinte e três diplomas no período 25/07/2019 a 01/08/2019, no seguinte livro de registro e sequências numéricas: RDG-001 - registros 1680; 1719 a 1866; 1868 a 2028; 2029 a 2043.

A relação dos diplomas registrados poderá ser consultada em até quinze dias, no endereço http://online3.ucq.edu.br:8080/web/app/Edu/PortalEducacional/js/aluno/diploma/.

Quixadá - CE, 15 de agosto de 2019.
MARCOS JAMES CHAVES BESSA
Reitor

Fonte: adaptado de (BRASIL, 2018).

As IES vinculadas ao sistema de ensino brasileiro deverão adotar os procedimentos previstos nesta Portaria para fins de expedição e registro de diplomas. O registro do diploma representa que o aluno cumpriu todos os requisitos e procedimentos necessários para receber o título relacionado ao curso superior que frequentou. Os diplomas de cursos superiores reconhecidos quando registrados terão validade em todo território nacional como prova da formação recebida. Os diplomas expedidos pelas Universidades, Institutos Federais ou Centros Universitários serão por eles próprios registrados. No caso de Faculdades, o registro deve ser feito por uma instituição credenciada, como uma Universidade pública ou privada (BRASIL, 2018).

2.1.2 Acesso aos Diplomas no Ensino Superior

As IES também deverão manter banco de informações de registro de diplomas a ser disponibilizado no sítio eletrônico da IES, após realizado o devido registro no DOU. Com isso, os diplomas expedidos pelas universidades serão por elas próprias registrados e poderão determinar o fluxo do respectivo processo de registro, dentro dos limites de sua autonomia e

desde que observada a legislação vigente (BRASIL, 2018). Com essas novas regras, o governo brasileiro tem a intenção de melhorar os processos internos das instituições, dando agilidade e segurança às informações para entregar uma melhor experiência ao aluno.

Tendo como base as problemáticas informadas, a abordagem proposta baseada na tecnologia *blockchain* tem como finalidade criar um ambiente em que as IES possam publicar o extrato das informações de diplomas e também disponibilizar uma consulta ao banco de informações de registro dos diplomas. Essa arquitetura irá aproveitar a propriedade inalterável da *blockchain* e o princípio da verificabilidade dos dados para evitar a falsificação de certificados e otimizar o tempo de consulta da veracidade dos dados.

2.2 *Blockchain*

A tecnologia *blockchain* é uma das mais recentes inovações, que pode ser considerada um novo paradigma para a regulamentação das atividades humanas e empresariais. É um mecanismo de consenso distribuído para armazenar as informações das transações em uma rede *Peer-to-Peer* (P2P) (ISLAM *et al.*, 2020). De acordo com Gatteschi *et al.* (2018), existem as seguintes categorias de evolução da *blockchain*:

- *Blockchain* 1.0: desenvolvimento de criptomoedas, em que seu foco eram facilitar transações em dinheiro (por exemplo, o Bitcoin);
- *Blockchain* 2.0: introdução de aplicações que vão muito além de transações em dinheiro, ou seja, relacionadas a ações, empréstimos, hipotecas, títulos e contratos inteligentes;
- *Blockchain* 3.0: muitas aplicações foram desenvolvidas em vários setores, como governo, educação, saúde e ciências.

Essa tecnologia foi concebida como um projeto de código aberto para introduzir uma moeda digital (*criptomoeda*) chamada Bitcoin. Embora o conceito de *blockchain* tenha sido discutido pela primeira vez por meio do Bitcoin, ele tem casos de uso que vão muito além das *criptomoedas* (ISLAM *et al.*, 2020). De acordo com Greve *et al.* (2018), as principais propriedades que compõem a estrutura da *blockchain* são as seguintes:

- Descentralização: não existe uma entidade centralizadora controlando as aplicações e participantes da rede *blockchain*, ou seja, o controle da rede é distribuído e as transações são validadas através de um processo de consenso realizado entre os nós desse ambiente, sem a necessidade de uma entidade intermediária confiável;
- Disponibilidade e Integridade: a rede *blockchain* é composta por vários nós, em que os

dados das transações são replicados em cada nó de maneira segura. Dessa forma o sistema se mantém disponível e consistente;

- Transparência e Auditabilidade: o livro de registros das transações é público e todo mundo pode verificar os dados. Além disso, os códigos fontes da tecnologia são abertos, isso permite que o sistema seja transparente e auditável;
- Imutabilidade e Irrefutabilidade: após um dado ser registrado na *blockchain* se torna imutável, ou seja, não é possível realizar modificações no mesmo. Com isso, as transações não podem ser refutadas e atualizações podem ser possíveis através de novas transações;
- Privacidade e Anonimidade: não existe terceiros envolvidos com acesso ou controle dos dados dos usuários. Através dos mecanismos de assinatura digital e criptografia assimétrica (par de chaves pública e privada) as transações são até certo ponto anônimas, considerando o endereço dos envolvidos na *blockchain*;
- Desintermediação: a integração entre diversos sistemas de forma direta e eficiente é possível através dessa tecnologia, permitindo a eliminação de intermediários e simplificando o projeto dos sistemas e processos;
- Cooperação e Incentivos: oferece incentivos baseados na teoria dos jogos para cooperação entre os membros da rede.

Inicialmente a tecnologia *blockchain* ganhou popularidade à medida que foi vista como uma forma de se eliminar intermediários e descentralizar o sistema. Desde então, a *blockchain* teve um crescente interesse de diferentes domínios da sociedade. Frequentemente, *blockchain* é conhecida como uma nova espécie de banco de dados de sistemas, sendo essencialmente um ambiente para processamento de transações distribuídas em uma rede, em que os nós não são confiáveis (THAKKAR *et al.*, 2018). Os conceitos apresentados até então têm o propósito de entender a *blockchain*. No entanto, para estimar de uma melhor forma seu potencial é necessário analisar os aspectos de sua estrutura, aplicações e perspectivas. As próximas seções desse capítulo tratam dessas análises para compreender melhor cada especto dessa tecnologia.

2.2.1 Surgimento e Definição de Blockchain

Experimentos com cadeia de blocos criptograficamente protegida foram registrados pela primeira vez no trabalho de Haber e Stornetta (1991), em que o objetivo era desenvolver um sistema que os *timestamps* de documentos não pudessem ser adulteradas. Porém, foi apenas em 2008 que uma pessoa ou entidade sob o pseudônimo de Satoshi Nakamoto publicou um artigo

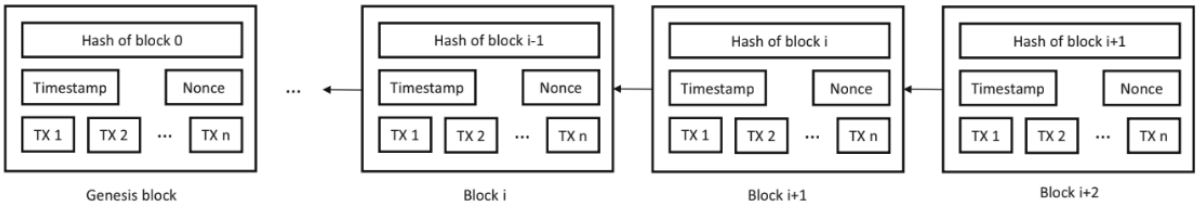
para introduzir o Bitcoin, uma *criptomoeda* baseada em uma moeda imutável e o razão público descentralizado que ficou conhecido como *blockchain* (NAKAMOTO, 2008).

A primeira *blockchain* conhecida foi a *blockchain* Bitcoin, que também é o nome da primeira *criptomoeda* descentralizada amplamente utilizada. Bitcoin também se refere ao protocolo de rede subjacente à *criptomoeda*. Em termos popular, a *blockchain* Bitcoin é automaticamente associada a *blockchain* quando, na prática, existem outras *blockchain* de importância significativa, como por exemplo, a *blockchain* da Ethereum (GRECH; CAMILLERI, 2017).

Blockchain é uma sequência de blocos que contém o registro completo de transações como um livro público, no qual é mantido por vários nós em uma rede (BHASKAR; CHUEN, 2015). Cada nó contém a cópia idêntica desse livro de registros (nesse trabalho será adotado essa tradução para *ledger*, porém pode ser traduzido também como livro-razão), sendo cada bloco uma sequência lógica de transações, que são registros permanentes, transparentes e imutáveis (THAKKAR *et al.*, 2018). Cada bloco contém um carimbo de data/hora (*timestamp*), o valor de *hash* que é computado usando um algoritmo de *hash* ou prova de trabalho conhecido (por exemplo, SHA-256, Ethash e Equihash) e o *hash* do bloco anterior chamado bloco pai, por fim um "*nonce*", que é um número aleatório para verificar o *hash* (NOFER *et al.*, 2017).

Este conceito garante a integridade de toda a *blockchain* até o primeiro bloco (bloco de gênese). Os valores do *hash* são únicos e fraudes podem ser efetivamente prevenidas, uma vez que as mudanças de um bloco na cadeia mudariam imediatamente o respectivo valor do *hash* (NOFER *et al.*, 2017). A Figura 3 representa uma *blockchain* no qual o bloco recém validado aponta para o bloco imediatamente anterior gerado. Cada bloco na cadeia confirma a integridade do anterior, e todo o caminho de volta ao primeiro bloco, denominado de bloco de gênese (BHASKAR; CHUEN, 2015).

Figura 3 – Exemplo de *blockchain* e seus blocos



Fonte: adaptado de (NOFER *et al.*, 2017).

A tecnologia *blockchain* pode registrar transações entre duas partes de forma eficiente e de maneira verificável e permanente, eliminando a necessidade de terceiros entre as partes.

Além disso, a disponibilidade de todas as transações concluídas para todos os nós torna um sistema baseado em *blockchain* mais transparente que as soluções centralizadas. As transações são validadas pelos nós membros usando um protocolo de consenso, o que garante que todos os nós tenham uma cópia idêntica da *blockchain*. Um novo bloco é considerado verificado somente após a maioria dos nós membros votar como verdadeiro e confiável usando o protocolo de consenso (BOSU *et al.*, 2019).

Não há controle central sobre a operação de uma *blockchain*. A filosofia é que nenhum participante ou grupo de participantes possa controlar a infraestrutura da *blockchain*. Todos os participantes da rede têm um papel igual a desempenhar (BOSU *et al.*, 2019). As novas transações não são automaticamente adicionadas ao livro de registros. Em vez disso, o processo de consenso garante que essas transações sejam armazenadas em um bloco por um certo tempo (por exemplo, 10 minutos na *blockchain* do Bitcoin) antes de serem transferidas para o livro de registros. Após este processo, as informações na *blockchain* não podem mais ser alteradas (NOFER *et al.*, 2017).

2.2.2 Estrutura da Blockchain

Visualizar o *blockchain* como um componente de software nos ajuda a entender os importantes impactos arquitetônicos sobre o desempenho e a qualidade de atributos como segurança, privacidade, escalabilidade e sustentabilidade. Como componente, a *blockchain* possui propriedades e limitações exclusivas. *Blockchains* são componentes de software complexos e baseados em rede, que podem fornecer armazenamento de dados, serviços de computação e serviços de comunicação (XU *et al.*, 2019).

2.2.2.1 Rede Peer-to-Peer

Redes *Peer-to-Peer* são frequentemente associadas à distribuição de arquivos de mídia, como áudio e vídeo. Em outros casos, a tecnologia é usada para distribuir grandes quantidades de dados, como no caso de atualizações de software, *backup* de serviços e sincronização de dados em vários servidores (STEEN; TANENBAUM, 2017). Essa tecnologia se tornou popular para esses fins, principalmente porque suporta um grande número de usuários (*Peers*) e requer um baixo custo operacional em comparação com outras opções, como o modelo tradicional baseado em cliente-servidor (MIGUEL, 2017). Sistemas que utilizam essa tecnologia permitem que os usuários acessem os dados armazenados em outros computadores conectados na mesma

rede P2P, no qual não é necessário um servidor centralizado. Exemplos de plataformas que usam essa tecnologia são BitTorrent e IPFS (*InterPlanetary File System*) (XU *et al.*, 2019).

A arquitetura P2P, portanto, tem o potencial de aumentar a confiabilidade e tolerância a falhas por causa de sua independência de servidores dedicados e centralizados ao controle. Por exemplo, uma rede P2P de *Voice-over-IP* (VoIP) pode iniciar e receber chamadas de voz de um ponto (*Peer*) para outro sem depender de servidores centralizados que podem se tornarem sobrecarregados (ZUO; IAMNITCHI, 2016).

Uma *blockchain* por definição é composta por uma rede P2P, em que cada máquina participante atua como um nó (*peer*) na rede, ou seja, a *blockchain* é uma rede descentralizada com vários nós conectados (RIFI *et al.*, 2017), em que os dados armazenados são replicados automaticamente ou com base no comportamento dos usuários na rede P2P (XU *et al.*, 2017). A natureza da topologia P2P na *blockchain* ajuda a compartilhar os recursos e reduzir os riscos de segurança (ALAMMARY *et al.*, 2019).

2.2.2.2 Criptografia

Para a segurança em sistemas distribuídos é fundamental o uso de técnicas de criptografia. A ideia básica de aplicar essas técnicas é simples. Considere um remetente S querendo transmitir a mensagem M para um receptor R. Para proteger a mensagem contra ameaças de segurança, primeiro o remetente criptografa M em um formato ininteligível, que posteriormente, envia M para R. O receptor R, por sua vez, deve descriptografar a mensagem recebida para ter acesso a sua forma original (STEEN; TANENBAUM, 2017).

A criptografia pode ser categorizada em dois tipos: simétrica (chave privada) ou assimétrica (chave pública). Na criptografia simétrica, a mesma chave é usada para criptografar e descriptografar uma mensagem. Essa tipo de criptografia também é chamada de chave secreta ou chave compartilhada, porque o remetente e o destinatário devem compartilhar a mesma chave e para garantir que a proteção funcione, sendo que essa chave compartilhada deve ser mantida em segredo. Essa condição de que ambas as partes possuam acesso à mesma chave secreta é uma das principais desvantagens da criptografia simétrica em comparação com a criptografia de chave pública, que utiliza duas chaves (pública e privada), ou seja, na criptografia assimétrica as chaves para criptografia e descriptografia são diferentes, mas juntas formam um par único. Uma das chaves na criptografia assimétrica é mantida privada, enquanto a outra é tornada pública. Por esse motivo, os sistemas criptográficos assimétricos também são chamados de sistemas de chave

pública (STEEN; TANENBAUM, 2017).

A criptografia apoia fortemente a *blockchain* para cumprir os requisitos de segurança do sistema e das aplicações. Dentre os recursos mais utilizados, destacam-se as funções *hash* e as assinaturas digitais (GREVE *et al.*, 2018).

De acordo com Ishmaev (2017), uma função *hash* é essencialmente uma função matemática que dada uma entrada de dados de qualquer tamanho, produz uma saída de tamanho limitado que pode ser computável com eficiência (em um período de tempo razoável). A função *hash* possui várias propriedades importantes, das quais as três seguintes são particularmente úteis para as implementações de *blockchains*:

- Primeiramente, a função *hash* é resistente à colisão, que significa que duas entradas distintas não produzem a mesma saída. Na prática, isso significa que a função *hash* pode ser usada como um resumo de mensagem, uma ferramenta para verificar se uma cópia de uma mensagem é idêntica ao original;
- A segunda propriedade é a ocultação, o que significa que dada apenas a saída, ninguém pode inferir o valor da entrada. Essa propriedade se traduz na aplicação de um compromisso de ligação, semelhante a colocar uma mensagem em um envelope e se comprometer com seu conteúdo sem revelá-lo. Depois que a mensagem é colocada no envelope, não é possível mudar de ideia e alterar seu conteúdo;
- A terceira propriedade é a facilidade de quebra-cabeça, o que significa que a função *hash* pode ser apresentada na forma de um quebra-cabeça matemático, onde tentamos diferentes entradas para uma determinada função *hash* para obter uma saída com um valor predeterminado.

A primeira e a segunda propriedades das funções *hash* são empregadas para construir estruturas de dados complexas usando estruturas de dados simples (ponteiros de *hash* como blocos de construção). A facilidade de quebra-cabeças não é um requisito necessário para uma estrutura de dados em si, mas é necessária para a *blockchain*. Um ponteiro é uma estrutura de dados, em que é essencialmente uma referência que indica onde as informações são armazenadas, semelhante ao código em um catálogo de biblioteca. O ponteiro de *hash*, por sua vez, é uma referência complementada com um breve resumo das informações a que se refere (útil para verificação). Usando ponteiros de *hash*, é possível construir uma estrutura de dados em forma de *blockchain*, formando uma cadeia de blocos que representa essa estrutura. Exemplos de funções *hash* que são usadas nas *blockchains* Bitcoin e Ethereum são SHA-256 e Keccak-256

respectivamente (ISHMAEV, 2017).

As assinaturas digitais se assemelham às assinaturas convencionais, atendendo às mesmas propriedades de assinaturas manuais em documentos. Assim, somente você é capaz de realizar a sua assinatura em um documento, porém qualquer um pode verificar a sua autenticidade. Além disso, não é possível o uso dessa mesma assinatura vinculada a outro documento diferente do original assinado, ou seja, não é possível forjar a sua assinatura, pois ela deve ser irrefutável. A utilização de assinaturas digitais tem como objetivo trazer a autenticidade e aprovação das informações transmitidas entre os participantes de uma rede (GREVE *et al.*, 2018).

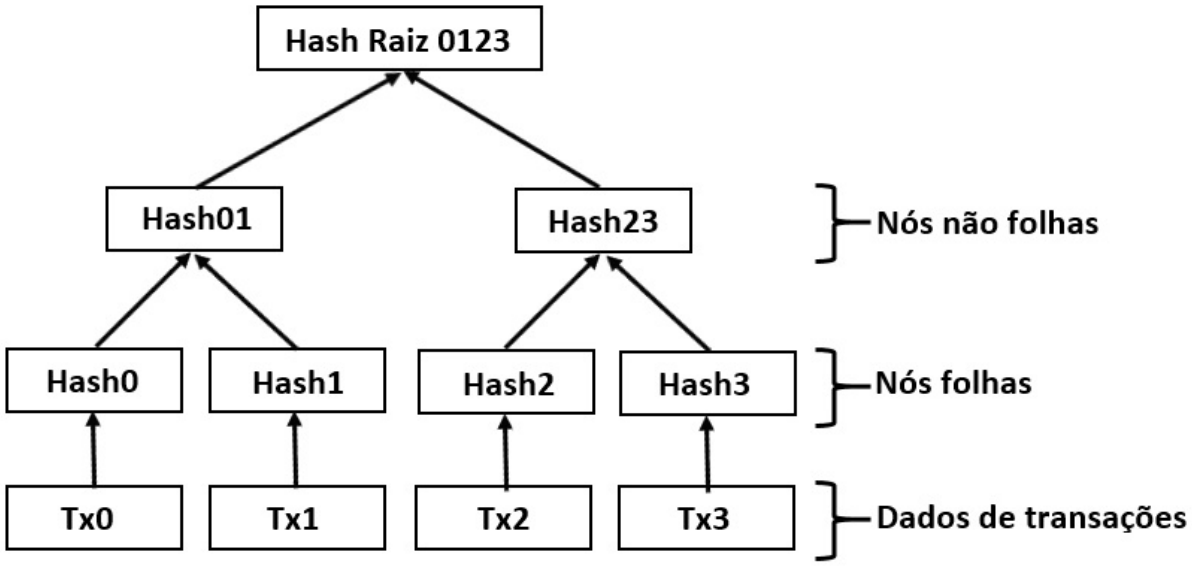
As assinaturas digitais são implementadas através de criptografia de chave assimétrica, em que além da chave privada (secreta) usada para assinar os documentos, também será utilizada uma chave pública, ou seja, a partir da chave pública e privada de um remetente será possível assinar e conferir a autenticidade de um documento. A chave privada será usada para encriptar, enquanto a chave pública será usada para decriptar. A encriptação a partir da chave privada, gera um código atrelado ao documento, que pode ser verificado ao se utilizar a chave pública para descriptografar. A chave privada é secreta e não deve ser revelada para ninguém, enquanto a chave pública deve ser revelada para qualquer um que queira atestar a autenticidade da assinatura. Criptografia, funções *hash* e assinaturas digitais são fundamentais para assegurar as propriedades de segurança da *blockchain* (GREVE *et al.*, 2018).

2.2.2.3 Árvore de Merkle

Uma Árvore Merkle é uma árvore de *hashes* construída de baixo para cima, conforme mostrado na Figura 4. Ela permite a verificação eficiente da integridade dos dados. Cada nó folha é um *hash* de dados (por exemplo, transações), e cada nó não folha é um hash de seus nós filhos, culminando no nó superior (ou seja, o *hash* raiz ou a raiz Merkle). Essa estrutura de dados otimiza o armazenamento e verificação de dados em um *blockchain*. Armazenamento de dados é otimizado porque apenas os *hashes* precisam ser salvos e o *hash* raiz é a impressão digital de todo o conjunto de dados. A verificação de dados é otimizada porque apenas uma pequena parte da árvore precisa ser percorrida a fim de verificar onde as alterações ocorreram (POPOVIC *et al.*, 2020).

O *hash* raiz é a impressão digital de todo o conjunto de dados, fazendo parte do cabeçalho do bloco na *blockchain*. Outro componente do mesmo cabeçalho do bloco é o *hash* do bloco anterior. Esta é uma estrutura de dados única, em que os blocos estão encadeados como

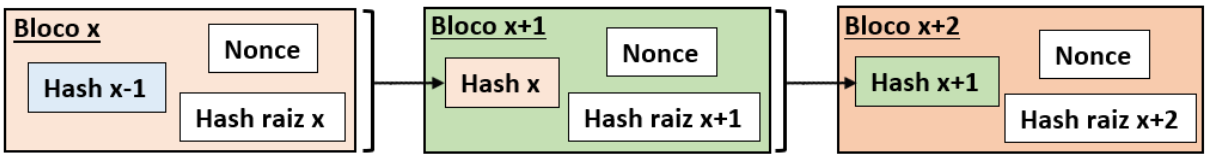
Figura 4 – Transações com *hash* em uma Árvore Merkle



Fonte: adaptado de (POPOVIC *et al.*, 2020).

mostrado na Figura 5, essa é uma das características dos recursos da *blockchain* que a torna inviolável. Isso ocorre porque uma mudança nos dados causaria uma mudança no *hash* do bloco, tornando-o incompatível com o cabeçalho do próximo bloco. Portanto, um adversário que deseja alterar o estado de um determinado bloco precisaria alterar todos os blocos. Em um mecanismo de consenso de prova de trabalho, isso exigiria mais da metade do poder de computação de toda a rede *blockchain* (conhecido como ataque de 51%) (POPOVIC *et al.*, 2020).

Figura 5 – Os estados anteriores estão ligados ao estado atual



Fonte: adaptado de (POPOVIC *et al.*, 2020).

2.2.3 Consenso

O consenso é um problema na computação distribuída em que os nós dentro do sistema devem chegar a um acordo dada a presença de processos defeituosos ou nós enganosos. Em *blockchain* as transações do livro de registros são verificadas por vários clientes ou "validadores" na rede ponto a ponto da *criptomoeda*, usando um dos muitos algoritmos de consenso que existem para resolver o problema de confiabilidade em uma rede envolvendo vários nós não confiáveis (BACH *et al.*, 2018). O objetivo de um algoritmo de consenso na *blockchain* é

garantir que todos os nós participantes concordam com as transações realizadas na rede, que formam um histórico que é serializado na forma de um blockchain (XIAO *et al.*, 2020). Os algoritmos de consenso mais amplamente usados são o algoritmo *Proof-of-Work* (PoW) e o algoritmo *Proof-of-Stake* (PoS), traduzidos como Prova de Trabalho e Prova de Participação respectivamente. No entanto, também existem outros algoritmos de consenso que utilizam implementações alternativas de PoW e PoS, bem como outras implementações híbridas e algumas estratégias de consenso totalmente novas (BACH *et al.*, 2018).

2.2.3.1 Problema do Gasto Duplo

O consenso em computação distribuída é uma forma mais sofisticada da realização do sistema distribuído. Em um sistema de computação distribuída típico, um ou mais clientes emitem solicitações de operações para um consórcio de servidores, que fornece serviço de computação correto e oportuno em resposta às solicitações, apesar de alguns servidores poderem falhar. Em comparação com a computação distribuída tradicional, uma rede *blockchain* permite que cada participante possa ser um cliente (para emitir transações) e um servidor (para validar e finalizar transações). Os dados do livro de registros subjacente a estrutura da *blockchain* são o alvo do consenso e consiste de blocos ordenados cronologicamente e encadeados por *hash*. Cada bloco contém um pacote de transações, sendo que as transações válidas em toda a *blockchain* devem ser consistentes entre si, ou seja, deve-se evitar gasto duplo ou excessivo (XIAO *et al.*, 2020).

Na lógica econômica das *criptomoedas* existe uma associação ao problema do gasto duplo, que representa um desafio de contabilidade e prestação de contas que as *criptomoedas* tentam superar de maneira eficaz. Esse problema é uma falha em potencial em uma *criptomoeda* ou outro esquema de dinheiro digital em que o mesmo *token* pode ser gasto mais de uma vez. Isto é possível porque um *token* digital consiste em um arquivo digital que pode ser duplicado ou falsificado (CHOHAN, 2017). O criador do Bitcoin, Satoshi Nakamoto, foi profundamente atento ao problema do gasto duplo e incluiu ele no artigo publicado que descreveu a implantação do Bitcoin (NAKAMOTO, 2008). Portanto, o problema do gasto duplo levanta questões sobre a proteção da moeda digital da mesma forma que as moedas tradicionais devem ser protegidas de fraudes ou falsificação, assim como também os problemas de responsabilidade subjacentes na proteção da informação digital (CHOHAN, 2017).

2.2.3.2 Algoritmo Proof-of-Work

O PoW é o algoritmo mais conhecido e implementado, sendo utilizado primeiramente na rede Bitcoin. Com a ajuda deste protocolo de consenso, Bitcoin se tornou o primeiro sistema de moeda digital a resistir a ataques de gasto duplo em um sistema descentralizado ponto a ponto de uma rede de pouca confiança. Esse protocolo é a chave por trás do Bitcoin e muitas outras *criptomoedas* estabelecidas como Ethereum e Litecoin (XIAO *et al.*, 2020).

No algoritmo Prova de Trabalho a geração de blocos na *blockchain* requer encontrar uma pré-imagem para uma função *hash* para que o resultado do *hash* satisfaça uma meta de dificuldade definida, que é ajustada dinamicamente para manter um intervalo médio de geração de blocos. Também qualquer transação ou bloqueio gerado deve ser anunciado imediatamente e transmitido para todos nós da rede. Um bloco ou transação precisa ser validado antes de ser transmitido para os nós da rede ou anexado a *blockchain*. A validação inclui verificar o gasto duplo e a validade da prova de trabalho no cabeçalho do bloco. No PoW é considerada a cadeia mais longa para representar a rede de consenso, que deve ser aceita por qualquer nó (também chamado de minerador) que participa dessa rede. A mineração deve sempre estender a cadeia mais longa (XIAO *et al.*, 2020).

Nesta abordagem, funciona como uma competição em termos de computação, em que os mineradores competem para resolver um problema criptográfico que consiste em encontrar um valor que concatenado junto com outros dados do bloco (por exemplo, dados das transações, *timestamps* e *hash* do bloco anterior) é passado como entrada para uma função *hash* (por exemplo, SHA-256, Ethash e Equihash), que tenta encontrar um número aleatório chamado "*nonce*" que vai sendo incrementado até satisfazer as condições para resolver a função *hash* do próximo bloco. Quando as condições são satisfeitas um novo bloco é minerado. Na geração de um bloco os mineradores podem reivindicar uma certa quantidade de novos *tokens* e taxas coletadas de todas as transações incluídas, na forma de uma transação para si mesmo como recompensa pelo trabalho realizado (XIAO *et al.*, 2020).

O poder computacional desse algoritmo vem do investimento real em hardware e as taxas de transações são usadas para incentivar os mineradores a participar honestamente e injetar novas moedas em circulação. À medida que a rede Bitcoin continua a crescer, o algoritmo de consenso PoW encontrou gargalos de desempenho e problemas de sustentabilidade. Em resposta às limitações de desempenho no PoW, os pesquisadores da *blockchain* têm investigado novos mecanismos, como os algoritmos de Prova de Participação, Prova de Autoridade (*Proof-*

of-authority (PoA)) e Prova do Tempo Decorrido (*Proof-of-Elapsed-Time* (PoET)), que não requerem mineração intensiva de computação, portanto, de forma eficaz reduzem o consumo de energia. Em alguns casos, métodos criptográficos podem ser usados para estabelecer confiança entre os nós, permitindo o uso de esquemas de proposição de blocos mais coordenados e continuar com incentivos apropriados para encorajar a participação na rede *blockchain*, pois esse é um componente chave do protocolo de consenso. Portanto, propostas de esquemas de blocos alternativos são frequentemente acompanhadas por um novo mecanismo de incentivo que promove justiça de participação e aumenta sustentabilidade geral do sistema (XIAO *et al.*, 2020).

2.2.3.3 Algoritmo Proof-of-Stake

O PoS se origina da comunidade Bitcoin como uma alternativa eficiente em termos de energia à mineração do PoW. Em termos mais simples, é uma participação que refere-se às moedas ou aos *tokens* da rede de propriedade de um participante que podem ser investidos no processo de consenso da *blockchain*. Do ponto de vista da segurança, o PoS aproveita a propriedade do *token* para mitigação de ataques Sybil (ameaça ao sistema em que tentam assumir o controle da rede criando múltiplas contas). Comparado a um minerador do PoW, cuja chance de gerar um bloco é proporcional ao seu poder de computação de força bruta, a chance de gerar um bloco para um minerador no PoS é proporcional ao seu valor de participação na rede (XIAO *et al.*, 2020).

Do ponto de vista econômico, o PoS move o custo de oportunidade de um minerador de fora do sistema (desperdício de poder de computação e eletricidade) para dentro do sistema (perda de capital e ganho de investimento). Por causa da falta real de mineração, muitas vezes nos referimos a um minerador no PoS como um validador, ou uma parte interessada pela grande semelhança do PoS com o investimento em mercados capitais (XIAO *et al.*, 2020).

As principais variações do PoS seguem a estrutura do consenso do PoW, em que a comunicação ocorre por mensagens. Existem as regras de validação de bloqueio, as regras de cadeia mais longa e finalidade probabilística. Ao contrário do PoW, um minerador do PoS pode tentar resolver o quebra-cabeça do *hash* apenas uma vez por ciclo de tentativas. Com isso, a dificuldade do quebra-cabeça diminui com o valor da participação do validador. O número de tentativas para resolver o problema do quebra-cabeça do *hash* pode ser significativamente reduzido se o valor da participação do minerador for alto. Portanto, o PoS evita a competição de força bruta que ocorreria se PoW fosse usado. Dessa forma é alcançando uma significativa

redução do uso de energia. Os primeiros sistemas de *blockchain* baseados no PoS foram Peercoin e Nxt (XIAO *et al.*, 2020).

2.2.4 Tipos de Blockchain e Plataformas

A questão de determinar que tipo de *blockchain* e qual configuração usar no desenvolvimento de soluções tem apresentado um grande obstáculo na tomada de decisão entre fabricantes e arquitetos de sistemas. Mesmo tendo uma estrutura para abordar essas questões e explicar de forma abrangente o projeto técnico e considerações sobre as aplicações de negócios, eles falham em abordar as comuns tomadas de decisão para verificar se uma solução *blockchain* é viável, e no caso de sim, que tipo de *blockchain* deve ser implementada. Cada implementação de uma *blockchain* requer uma análise cuidadosa para decidir com base nas características individuais da aplicação (PEDERSEN *et al.*, 2019).

Pedersen *et al.* (2019) relataram a existência de três tipos de *blockchain*:

– A *blockchain* pública sem permissão é uma rede aberta que permite a participação de qualquer pessoa (exemplos incluem Bitcoin e Ethereum). Com esse tipo de *blockchain*, todos os usuários podem ler, escrever e verificar transações. Esse tipo de *blockchain* pode substituir o papel de um terceiro confiável. A confiança é construída entre pares na rede, porque todos eles têm que respeitar o estabelecido mecanismo de consenso. Os mais populares mecanismos de consenso são o PoW e o PoS.
– A *blockchain* pública permissionada é uma rede fechada, em que apenas nós verificados e confiáveis podem participar (exemplos são Ripple, Multichain, Eris e Hyperledger Fabric). Esse tipo também é chamado de "*blockchain* híbrida", porque todos os participantes podem visualizar os dados, mas apenas usuários autorizados podem validar as transações. Os usuários são autorizados através de um consenso de rede depois de fornecer a prova necessária de elegibilidade.
– A *blockchain* privada permissionada é uma rede fechada que permite apenas usuários autorizados a ler, enviar e validar as transações (exemplos incluem Hyperledger Fabric e Corda). As transações são verificadas ou o consenso da *blockchain* é determinado dentro de uma organização. Geralmente é utilizado um protocolo de *Byzantine Fault Tolerance* (BFT), o qual requer uma certa porcentagem de nós previamente verificados para confirmar as transações.

Para iniciar o desenvolvimento de um projeto com *blockchain* em qualquer domínio

da sociedade, outra etapa importante é selecionar a plataforma mais adequada. As plataformas Bitcoin, Ethereum e Hyperledger Fabric são consideradas as mais conhecidas e utilizadas (XU *et al.*, 2019).

A utilização da plataforma Bitcoin consiste em seu livro de registros públicos, que é partilhado por todos os participantes na rede e que contém um registo ordenado das transações enviadas entre os mesmos. Cada transação representa um processo de transferência de valor entre duas carteiras Bitcoin (armazena as *criptomoedas* dos nós na rede), em que após a realização da transação é atualizado o saldo das carteiras, considerando que as transações são verificadas e validadas pelo mecanismo de consenso PoW (SINGHAL *et al.*, 2018). A rede da *blockchain* Bitcoin é pública, ou seja, qualquer pessoa pode participar da rede, para tanto, essa plataforma utiliza uma gerência de identidades descentralizada para atribuição de endereços aos nós da rede. Com isso, não existe uma única autoridade centralizadora responsável por emitir novas identidades (endereços), pois cada nó de forma independentemente, gera a sua própria identidade e a anuncia para os demais nós da rede quando necessário. Essa descentralização permite que a *blockchain* do Bitcoin ofereça uma rede cujas transações ocorrem de maneira pseudo-anônima, ou seja, conhece-se os endereços dos emissores e receptores dos ativos, mas não se sabe exatamente quem são, pois os endereços não estão ligados a um nome universal ou endereço *Internet Protocol* (IP). Essa pseudo anonimidade é um dos princípios básicos do Bitcoin (GREVE *et al.*, 2018).

Existem outras plataformas de *blockchain* públicas além da apresentada com o Bitcoin (focada na transferência de valores financeiros entre contas). Uma delas é a Ethereum, que expandiu o conceito de transações de acordo com suas aplicações, sendo possível o desenvolvimento de *Decentralized Application (DApp)*, alocadas na *blockchain*. Essa plataforma apresentou uma *blockchain* mais generalizada, expandindo as transações para operações computacionais chamadas de *smart contracts* (contratos inteligentes). A Ethereum também é uma das plataformas públicas de *blockchain* mais conhecidas, que pode oferecer suporte a contratos inteligentes avançados e personalizados com ajuda da linguagem de programação de *Turing* completa. A plataforma Ethereum pode suportar *loops*, contratos financeiros e jogos. Os códigos dos contratos inteligentes da Ethereum são escritos em um *bytecode* baseado em pilha e executado na *Ethereum Virtual Machine (EVM)*. Atualmente, a Ethereum é a plataforma mais comum para o desenvolvimento de contratos inteligentes (ALHARBY; MOORSEL, 2017).

A plataforma Hyperledger Fabric é uma *blockchain* de código aberto voltada para

aplicações empresariais, que tem um projeto modular e um alto grau de especificabilidade por meio de modelos confiáveis e componentes conectáveis (THAKKAR *et al.*, 2018). Essa plataforma está sendo usada em muitos casos de uso diferentes, como *Global Trade Digitization* (WHITE, 2018), *SecureKey* (SECUREKEY, 2017) e *Everledger* (EVERLEDGER, 2018). A Hyperledger é mantida pela Linux Foundation e diversas corporações, dentre elas a IBM. Nessa plataforma é possível a execução de DApp, desenvolvidas em linguagens de programação conhecidas e consolidadas no mercado, como por exemplo Go, Java ou Node.js. Uma aplicação descentralizada tem como base os contratos inteligentes, em que no contexto da plataforma Hyperledger Fabric, compreendidos como o código que implementa a lógica da aplicação (ANDROULAKI *et al.*, 2018). Essa plataforma é uma implementação de uma *blockchain* privada com objetivo de atender a variados requisitos de negócios. Sua arquitetura modular oferece confiabilidade, resiliência, flexibilidade e escalabilidade, permitindo a criação de vários módulos conectáveis e viabilizando a implantação de serviços diferenciados (GREVE *et al.*, 2018).

Semelhante ao Hyperledger Fabric, existe a plataforma Corda que tem um livro de registros compartilhados apenas entre grupos definidos de participantes da rede. Isso visa melhorar a privacidade e escalabilidade, reduzindo a replicação de dados na rede. Também existe a plataforma Ripple, que é considerada um sistema de liquidação e câmbio em tempo real entre instituições financeiras. A Ripple usa um livro de registros comum que é gerenciado por uma rede de servidores de validação independente que comparam constantemente registros de transações, no qual esses servidores de validação podem pertencer a indivíduos ou bancos. Várias técnicas foram propostas para preservar a privacidade na *blockchain*. Por exemplo, a plataforma Zcash criptografa informações de transações de pagamento e usa um método criptográfico para permitir que qualquer nó verifique a validade das transações criptografadas, permitindo que a rede *blockchain* tenha um livro de registros que possibilite pagamentos privados sem a divulgação das partes ou valores envolvidos. A plataforma Monero também dar ênfase a privacidade, em que usa outras ferramentas criptográficas para proteger endereços de envio e recebimento de valores das transações (XU *et al.*, 2019).

Existem várias outras plataformas para desenvolvimento com *blockchain*, em que grande parte tem propósitos e definições semelhantes aos apresentados, sendo necessário uma análise da infraestrutura e detalhes de implementação para escolher a plataforma mais adequada para determinado projeto (XU *et al.*, 2019).

2.3 Contratos Inteligentes

O conceito de contrato inteligente foi introduzido por Nick Szabo em 1994, em que definiu o mesmo como um protocolo de transação computadorizado que executa os termos de um contrato. Szabo sugeriu traduzir cláusulas contratuais (por exemplo, garantias e títulos) em código e incorporá-las em propriedades (hardware ou software) que possam se autoaplicar, de modo a minimizar a necessidade de intermediários confiáveis entre as partes envolvidas na transação, e a ocorrência de exceções maliciosas ou acidentais (SZABO, 1994).

Um contrato inteligente é uma aplicação autônoma com entradas e saídas pré-definidas que podem ser executadas por um minerador de maneira determinística. Qualquer usuário pode invocar um contrato inteligente, cujo resultado é registrado como uma transação no livro de registro distribuído (WOOD, 2019).

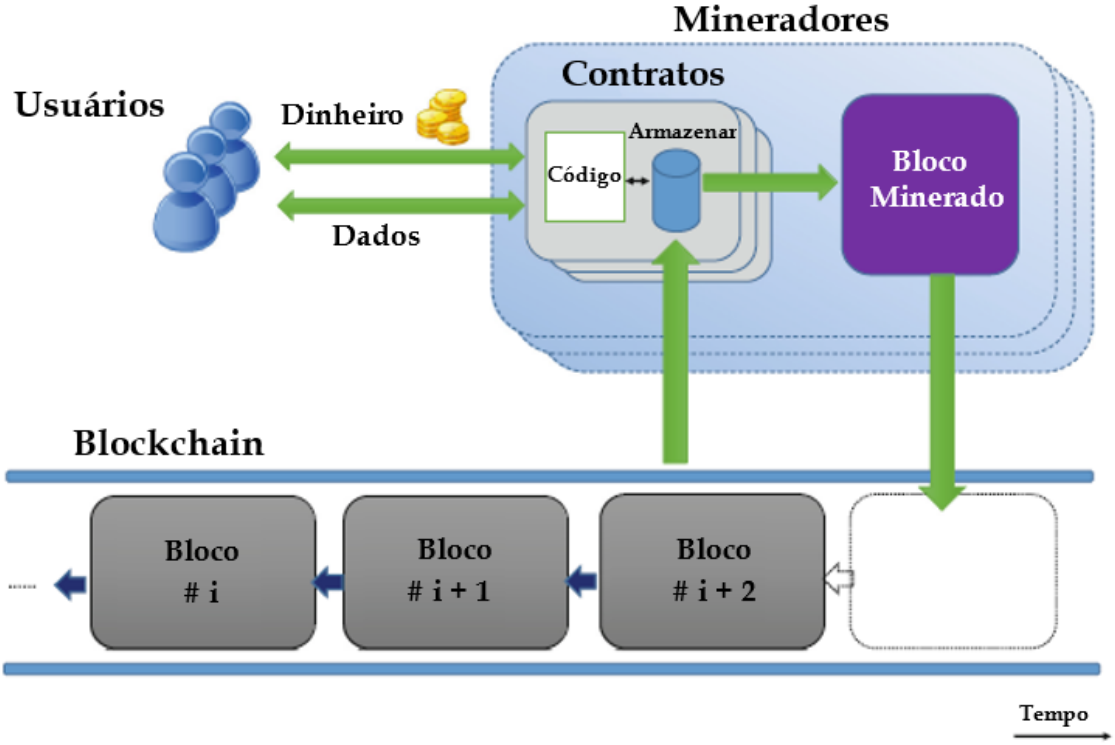
Os contratos inteligentes funcionam como *scripts* armazenados. Como residem na cadeia, eles têm um endereço exclusivo. Pode-se acionar um contrato inteligente endereçando uma transação para ele, em seguida, ele executa de forma independente da forma que foi escrito, em qualquer nó da rede, de acordo com os dados que foram incluídos no acionamento da transação (CHRISTIDIS; DEVETSIKIOTIS, 2016).

Os contratos inteligentes são criados sobre uma plataforma de *criptomoeda*, por exemplo a Ethereum. Uma *criptomoeda* é um sistema descentralizado para interagir com dinheiro virtual em um livro de registros compartilhado de forma global. Os usuários transferem dinheiro e interagem com contratos através da publicação de dados assinados que são chamados de transações da rede de *criptomoedas*. A rede consiste em nós chamados mineradores que propagam informações, armazenam dados, e atualizam os dados aplicando transações (DELMOLINO *et al.*, 2016).

Um esquema de alto nível é mostrado na Figura 6, no qual o estado de um contrato inteligente é armazenado em uma *blockchain*, sendo executado por uma rede de mineradores que chegam a um consenso sobre o resultado da execução, e atualizam o estado do contrato na *blockchain*, podendo os usuários enviar ou receber dinheiro ou dados do contrato. O código do contrato é executado sempre que recebe uma mensagem, de um usuário ou de outro contrato. Qualquer usuário pode criar e publicar um contrato através de uma transação na *blockchain*. O código da programação de um contrato é fixado quando o contrato é criado e não pode ser mais alterado (DELMOLINO *et al.*, 2016).

Como forma de visualizar com mais detalhes a Figura 6, será apresentado o ciclo

Figura 6 – Esquema de sistema de criptomoeda com contratos inteligentes



Fonte: adaptado de (DELMOLINO *et al.*, 2016).

de vida de um contrato inteligente de acordo com Sillaber e Waltl (2017), que cita as seguintes fases:

– Criação: essa fase pode ser dividida em negociação e implementação. Primeiramente, as partes (usuários) devem concordar com o conteúdo e os objetivos do contrato. Isso pode ser feito *online* ou *offline*, sendo semelhante as negociações clássicas de contratos existentes na sociedade. Todas as partes devem ter uma carteira de *criptomoeda* (para transferir dinheiro ou dados) na plataforma de *blockchain* utilizada. O identificador de cada usuário é um endereço criptografado, em que é usado para a identificação das partes e transferência de fundos. Depois de concordarem com os objetivos e conteúdo do contrato, o acordo deve ser transformado em código. A codificação do contrato é limitada pela expressividade da linguagem de programação usada. Para validar a execução de um contrato inteligente a maioria dos ambientes utilizados fornecem a infraestrutura para criar, manter e testar o contrato. A transformação de requisitos em código pode requerer várias iterações entre as partes interessadas e desenvolvedores até a fase de implantação do contrato inteligente. Depois que as partes envolvidas concordarem com a versão codificada do contrato, ele é enviado ao livro de registros distribuídos para publicação na rede *blockchain*. Durante esta fase, os nós participantes recebem o contrato como um bloco de transação, em que após

a confirmação (processo de mineração e consenso) pela maioria dos nós, o contrato está pronto para execução. Os contratos inteligentes não podem ser modificados após aceitação da rede, ou seja, mudanças não são possíveis e requerem a criação de um novo contrato.

- Congelamento: após o contrato inteligente ser enviado para *blockchain* e para prevenir uma inundação de contratos no ecossistema *blockchain*, uma taxa tem que ser paga aos mineradores. Deste ponto em diante, o contrato e todas as partes são públicas e acessíveis por meio do livro de registros público. Durante a fase de congelamento as transferências feitas para o endereço da carteira do contrato inteligente estão sendo congeladas e os nós assumem a função de um conselho de governança, garantindo que as condições prévias sejam cumpridas para a execução do contrato.
- Execução: os contratos armazenados na *blockchain* estão disponíveis para serem lidos pelos nós da rede. A integridade do contrato é validada e o mecanismo do ambiente (compilador e interpretador) executa o código do contrato. As entradas para a execução dos contratos são coletados dos oráculos inteligentes e partes envolvidas. A execução do contrato inteligente resulta em um conjunto de novas transações e um novo estado do contrato inteligente. Esse conjunto de resultados e o novo estado do contrato são enviados para o livro de registros distribuído e são validadas através do protocolo de consenso.
- Finalização: após o contrato inteligente ser executado, o resultado das transações e as novas informações de estado são armazenadas na *blockchain* e confirmadas de acordo com o protocolo de consenso. Os ativos digitais previamente comprometidos são transferidos e com a confirmação de todas as transações o contrato inteligente tem seu objetivo cumprido.

Existem dois tipos de contratos inteligentes, os determinísticos e não determinísticos. Um contrato determinístico é um contrato inteligente que, quando executado, não exige qualquer informação de uma parte externa (fora da *blockchain*). Um contrato não determinístico é um contrato que depende de informações de uma parte externa. Por exemplo, um contrato que exige que as informações meteorológicas atuais sejam executadas, ou seja, essa regra de negócio não está definida na *blockchain* (ALHARBY; MOORSEL, 2017).

Contratos inteligentes podem ser desenvolvidos e implantados em diferentes plataformas de *blockchain* (por exemplo, Ethereum, Bitcoin e NXT). Elas oferecem recursos distintos para o desenvolvimento de contratos inteligentes, sendo que algumas plataformas suportam linguagens de programação de alto nível para desenvolver contratos inteligentes. A plataforma Bitcoin é uma das *blockchains* públicas mais conhecidas para processar transações com *cripto-*

moedas, porém com uma capacidade de computação muito limitada. Ela usa uma linguagem de *script* de *bytecode* baseada em pilha. No Bitcoin, uma lógica simples requer várias assinaturas para assinar uma única transação antes de confirmar um possível pagamento. Em relação a criação de contratos inteligentes com lógica mais complexa não é possível, devido às limitações da linguagem de *script* Bitcoin. A linguagem de *script* Bitcoin, por exemplo, não suporta *loops*, sendo que a única maneira possível de implementar é repetindo o código várias vezes, o que é ineficiente (ALHARBY; MOORSEL, 2017). A plataforma Ethereum implementa alguns conceitos apresentados no Bitcoin, sendo acrescentada algumas melhorias na sua adaptabilidade e flexibilidade, permitindo o desenvolvimento para a realização de tarefas com certa complexidade computacional (SINGHAL *et al.*, 2018).

As melhorias e inovações tecnológicas fizeram o sonho dos anos 90 de ter contratos inteligentes descentralizados possível. Contratos (direitos e obrigações em geral) agora podem ser escritos em código, que é executado sem autoridade central e que podem ser analisados por qualquer pessoa que participe do livro de registros público. A descentralização de contratos inteligentes prometem trazer mudanças em vários domínios da sociedade (SILLABER; WALTL, 2017).

2.4 Ethereum

Ethereum é uma plataforma de código aberto e descentralizada lançada em 2015, podendo suportar várias aplicações derivadas de sua estrutura. Se a *blockchain* do Bitcoin for considerada uma rede global de pagamentos, a Ethereum seria um sistema de computação global. A Ethereum é uma plataforma semelhante a Android (desenvolvido pelo Google). Ela fornece uma infraestrutura que permite que os desenvolvedores criem aplicações. Essa infraestrutura é desenvolvida e mantida pela Ethereum e por esses desenvolvedores (CHENG *et al.*, 2018). Segundo Cheng *et al.* (2018), as principais características da Ethereum são: (i) terceiros não podem modificar nenhum dado, ou seja, incorruptível; (ii) os erros derivados de fatores pessoais são evitados porque as aplicações descentralizadas são mantidas por entidades em vez de indivíduos, fornecendo a segurança; e (iii) a *blockchain* não deixa de funcionar, mesmo se um computador individual ou servidor falhar, ou seja, é operacionalmente permanente.

A plataforma Ethereum possui a EVM que é uma *blockchain* programável. A EVM permite que os desenvolvedores executem qualquer programa da maneira que desejar. Os desenvolvedores instruem a EVM a executar aplicações usando uma linguagem de alto nível

chamada Solidity, que é fortemente tipada, com bibliotecas, herança e orientação a objetos. Anteriormente, eram usadas Mutan, LLL e Serpent, mas estas linguagens estão quase extintas. Solidity tem semelhanças com JavaScript, e sua mais nova alternativa é chamada Vyper, que se parece com Python. Porém, Solidity é a mais utilizada pela rede Ethereum. Essa linguagem de programação é usada para implementar contratos inteligentes, em que após a conclusão de uma programação de um contrato usando Solidity, um compilador chamado "solc" é necessário para transformar o código Solidity no *bytecode* do contrato, que é então interpretado pelo EVM. Em seguida, as instruções compiladas são implantadas em uma *blockchain* Ethereum (CHENG *et al.*, 2018).

A Ethereum possui suas próprias características e parâmetros de bloco, no qual fornece a capacidade de criar uma *blockchain* privada para fins de estudo e teste. Uma das formas de realizar essa criação é usando o *go-Ethereum* (Geth) como cliente para se conectar a *blockchain* Ethereum. Como interface para interagir com a *blockchain*, uma abordagem de aplicação *web* usando HTML e Javascript podem serem utilizadas para desenvolver um *front-end* para interação em uma rede de nós configurados em uma *blockchain* Ethereum privada ou pública (RIFI *et al.*, 2017).

Essa plataforma foi escolhida para o desenvolvimento do projeto deste trabalho devido ser atualmente a principal plataforma que trabalha com contratos inteligentes, possuindo uma comunidade ativa de desenvolvedores (SINGHAL *et al.*, 2018). Também foi escolhida devido às características relacionadas ao processamento das transações e protocolo de consenso. Além disso, existem diversas ferramentas e material didático disponível de fácil acesso na internet.

Na Ethereum, existem algumas redes de testes (*testnets*) públicas para os desenvolvedores criarem e validarem seus contratos inteligentes sem gastar *ethers* (*criptomoeda* da Ethereum para executar contratos) reais. Assim, os desenvolvedores usam *ethers* falsos para simular os custos e comportamento dos contratos antes da implantação na rede principal (*mainnet*) da Ethereum (SINGHAL *et al.*, 2018). Este trabalho utilizou a rede pública de testes *Ropsten* que utiliza o protocolo de consenso PoW, que representa a realidade atual mais próxima da rede principal da Ethereum.

2.4.1 Conceitos Elementares

A Ethereum se tornou a *blockchain* programável líder mundial para o desenvolvimento de aplicações descentralizadas. Como outras *blockchains*, a Ethereum tem uma *criptomoeda* nativa chamada *ether*. Diferente de outras *blockchains*, a Ethereum é programável usando uma linguagem *Turing* completa, ou seja, desenvolvedores podem codificar contratos inteligentes que controlam o valor digital, executado exatamente como programado e são imutáveis. Um contrato inteligente é basicamente uma coleção de códigos (suas funções) e dados (seu estado) que residem em um endereço específico na *blockchain* Ethereum. Contratos inteligentes na *blockchain* Ethereum são medidos usando *gas*. O *gas* é uma unidade que mede a quantidade de esforço computacional que levará para executar cada operação. Cada operação na Ethereum, seja uma transação ou execução de uma instrução de um contrato inteligente, requer alguma quantidade de *gas*. Os mineradores recebem uma quantia em *ether* que é equivalente ao quantidade total de *gas* necessária para executar uma operação completa na *blockchain* Ethereum (ALBERT *et al.*, 2020).

2.4.1.1 Gas e Ether

A fim de evitar problemas de abuso de rede e contornar as questões inevitáveis decorrentes da integridade de *Turing*, toda a computação programável na Ethereum está sujeita a taxas. Assim, qualquer dado ou fragmento de computação programável (isso inclui a criação de contratos, chamadas de mensagens, utilizando e acessando o armazenamento da conta e executando operações na máquina virtual) tem um custo universalmente acordado em termos de *gas* (WOOD, 2019).

Existem três justificativas para medição de *gas* no ambiente da Ethereum: (i) pagar pelo *gas* no momento de propor a transação evita que o emissor desperdice o poder computacional dos mineradores por exigir que realizem trabalho intensivo sem valor; (ii) taxas de *gas* desincentivam os usuários a consumir muito do armazenamento replicado, que é um recurso valioso em um sistema de consenso baseado em *blockchain*; e (iii) limita o número de cálculos que uma transação precisa para ser executada, portanto, evita ataques *Denial Of Service* (DoS) baseados em execuções sem término (ALBERT *et al.*, 2020).

Cada transação possui uma quantidade específica de *gas* associada, podendo ser um "gasLimit", que é a quantidade de *gas* comprada implicitamente do saldo da conta do remetente.

A compra acontece de acordo com o “gasPrice” especificado na transação. A transação é considerada inválida se o saldo da conta não suportar tal compra. É denominado “gasLimit”, uma vez que qualquer *gas* não utilizado no final da transação é reembolsado (na mesma taxa de compra) para a conta do remetente. O *gas* não existe fora da execução de uma transação. Assim, para contas com código confiável associado, um valor relativamente alto de limite de *gas* pode ser definido e deixado como parâmetro no código (WOOD, 2019).

Em geral, o *ether* é utilizado para comprar *gas*, que não é reembolsado. O endereço de uma conta normalmente está sob o controle de um minerador. As entidades (ou seja, não mineradores) que realizam transações são livres para especificar qualquer preço do *gas* que desejarem utilizar. No entanto, os mineradores são livres para ignorar as transações como eles escolhem. Um preço de *gas* mais alto em uma transação, custa mais para o remetente em termos de *ether* para entregar um valor maior para o minerador. Com isso, será mais provável o interesse de mais mineradores para selecionar a transação para inclusão no seus processos de mineração. Mineradores, em geral, anunciam o preço mínimo do *gas* para o qual eles executarão as transações e os operadores estarão livres para examinar esses preços na determinação do preço do *gas* para oferta. Uma vez que haverá uma distribuição (ponderada) de preços mínimos de *gas* aceitáveis, as entidades que realizam transações necessariamente têm um compromisso de reduzir o preço do *gas* e maximizar a chance de que sua transação seja explorada em tempo hábil (WOOD, 2019).

2.4.1.2 Transações

As transações são uma estrutura de dados atômica de uma *blockchain*. Normalmente, uma transação é criada por um conjunto de usuários ou objetos autônomos (contratos inteligentes) para indicar a transferência de *tokens* dos remetentes para os destinatários especificados. Uma transação especifica uma lista de entradas associadas aos valores de *token* com as identidades (endereços) das entidades de envio (WANG *et al.*, 2019).

A transação é uma única instrução assinada criptograficamente construída por um ator externo ao escopo da Ethereum. Embora se presuma que o ator externo final será de natureza humana, ferramentas de software serão utilizadas em sua construção e disseminação. Existem dois tipos de transações: aquelas que resultam em chamadas de mensagens e aquelas que resultam na criação de novas contas com código associado (conhecido como criação de contrato) (WOOD, 2019).

Para proteger a autenticidade de um registro de transação, as funcionalidades de criptografia *hash* e criptografia assimétrica são utilizadas. A função *hash* criptográfica mapeia aleatoriamente uma entrada binária de comprimento arbitrário para uma única saída binária de comprimento fixo. Com uma função *hash* segura (por exemplo, SHA-256), é computacionalmente inviável recuperar a entrada da imagem de saída. Além disso, a probabilidade de gerar a mesma saída para quaisquer duas entradas diferentes é insignificante (WANG *et al.*, 2019).

Em relação a criptografia assimétrica, cada nó na rede blockchain gera um par de chaves privada e pública. A chave privada está associada a uma função de assinatura digital, que produz uma *string* de assinatura de comprimento fixo para qualquer comprimento arbitrário da mensagem de entrada. A chave pública está associada a uma função de verificação, que tem como entrada a mesma mensagem e a assinatura reconhecida para essa mensagem. A função de verificação só retorna verdadeiro quando a assinatura é gerada pela função de assinatura com o chave privada correspondente e a mensagem de entrada. Os nós da rede identificam suas chaves públicas, ou seja, o código *hash* de suas chaves públicas, como seus endereços permanentes (também conhecidas como suas pseudo-identidades) na *blockchain*. Cada tupla de entrada em uma transação é assinada pela conta de envio. Dessa forma, a rede é capaz de validar publicamente a autenticidade da entrada por meio da verificação da assinatura com base no endereço público do remetente (WANG *et al.*, 2019).

2.4.2 Mineração

Implementar a *blockchain* pode exigir muitos recursos. Um parâmetro importante para analisar a tecnologia *blockchain* é o próprio bloco, ou seja, o tamanho, o tempo necessário para mineração, em outros termos, o custo. Mineração é o processo de validação de um bloco na *blockchain*. O importante é o fato de ser necessário muito poder computacional para se tornar um minerador de *blockchain*. Mineradores são geralmente recompensados, por exemplo, em Bitcoin. A mineração pode afetar todo desempenho do sistema, é um conceito crítico que precisa ser levado em consideração (RIFI *et al.*, 2017).

A mineração na *blockchain* é um processo de resolução de um quebra-cabeça criptográfico com poder de computação, em que os mineradores podem encontrar um novo bloco para *blockchain*. Eles podem obter uma recompensa pelo bloco encontrado como forma de retribuir pelo seu poder de computação utilizado no processo de mineração (QIN *et al.*, 2018).

A maioria das análises na literatura sobre as estratégias de mineração dos nós de

consenso são apresentadas no contexto da rede Bitcoin baseada em PoW. Mesmo assim, elas podem ser prontamente estendidas a outros esquemas de estrutura de protocolos de consenso. Para o protocolo PoW, o incentivo monetário é a chave para garantir que a maioria dos nós (mineradores) que participam do consenso siga as regras de transição de estado da *blockchain* durante a competição para solucionar o quebra-cabeça criptográfico. Em redes *blockchain* sem permissão, o mecanismo de incentivo é construído sobre os esquemas de emissão e transferência de *tokens*. Em um típico protocolo baseado no PoW em uma rede *blockchain*, o vencedor na concorrência para criar um novo bloco ganha as taxas das transações aprovadas e obtém recompensa da emissão de *token*, por exemplo, a recompensa em Bitcoin para expandir a *blockchain* com o novo bloco. Por esta razão, o processo de competição de solucionar o quebra-cabeça é comparado ao processo de "mineração de ouro", já que lançando recursos na competição, os nós esperam receber recompensas monetárias transportadas pelos *tokens*. Como resultado, os participantes do consenso (os nós) são mais conhecidos como "mineradores" de bloco para o público (WANG *et al.*, 2019).

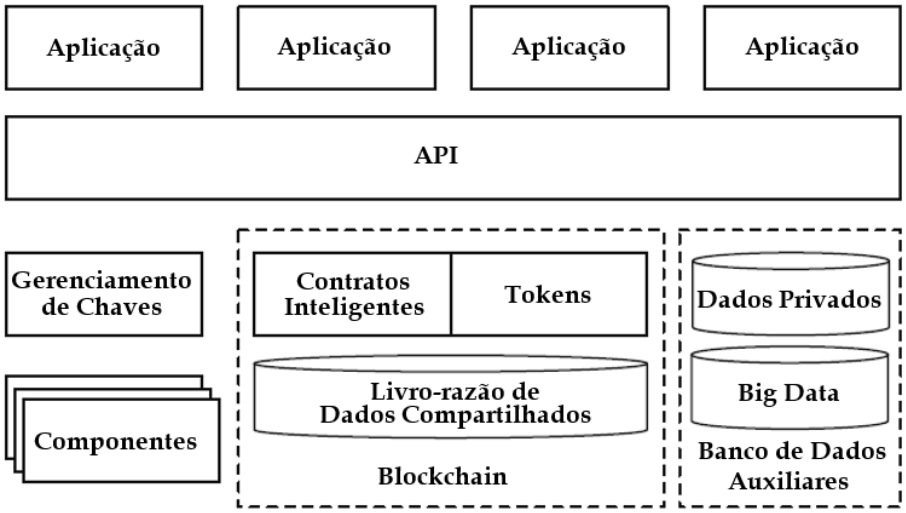
2.5 Arquiteturas para *Blockchain*

Na literatura, algumas arquiteturas foram propostas para *blockchain*. Muitas delas utilizam camadas para representar os elementos da arquitetura, sempre adicionando uma infraestrutura de *blockchain*. As arquiteturas apresentadas por Xu *et al.* (2018), Xu *et al.* (2019), Lu *et al.* (2018) e Wan *et al.* (2019) são exemplos identificados.

A Figura 7 exibe uma arquitetura de um sistema de software, proposta por Xu *et al.* (2018) e Xu *et al.* (2019), onde *blockchain* é um dos componentes. Nesse sistema, a *blockchain* é responsável por armazenar e compartilhar dados e executar contratos inteligentes. O componente *blockchain* também pode ter *tokens* como moedas digitais ou outros ativos. Devido às limitações de privacidade e desempenho, existem bancos de dados auxiliares fora da cadeia usados no sistema. Dados privados são armazenados em um banco de dados interno, e dados com tamanho grande são armazenados em um banco de dados separado, podendo ser um serviço em nuvem. Há uma camada *Application Programming Interface* (API) entre a camada de armazenamento de dados e os aplicativos que usam a *blockchain*, semelhante às tecnologias convencional. O gerenciamento de chaves é um componente essencial na *blockchain*, em que cada participante de uma rede *blockchain* possui uma ou mais chaves privadas, utilizadas pelo participante para assinar digitalmente as transações relativas aos endereços do participante. A segurança dessas

chaves privadas é muito importante. Se a chave privada de um usuário for roubada, qualquer outro usuário no sistema pode forjar transações desse usuário para gastar os ativos pertencentes ao usuário, ou invocar funções de contratos inteligentes em seu nome.

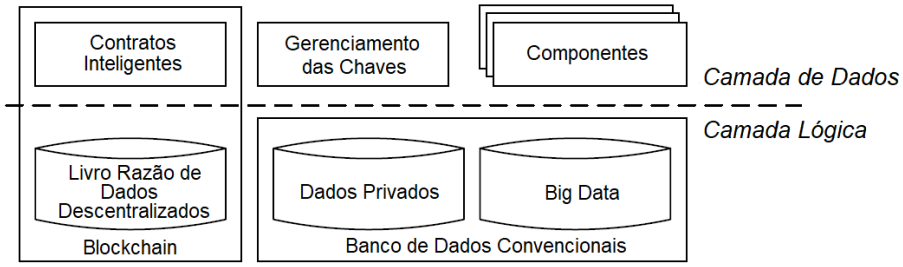
Figura 7 – *Blockchain* como um componente em uma arquitetura de software



Fonte: adaptado de (XU *et al.*, 2018)(XU *et al.*, 2019).

A Figura 8 exibe como a *blockchain* pode ser projetada como um componente de um sistema de aplicativo de software (LU *et al.*, 2018). Aplicativos *blockchain* consistem em uma camada lógica e uma camada de dados, como os aplicativos de software tradicionais. Na camada de dados, existem tipos de armazenamentos de dados nos quais os aplicativos de software podem ser construídos: dados que requerem integridade e / ou transparência e executar contratos inteligentes; e dados privados são armazenados em um banco de dados interno, enquanto dados grandes são frequentemente armazenados também em um armazenamento de dados separado, por exemplo, na nuvem. Assim, bancos de dados convencionais fora da cadeia são frequentemente necessários devido aos problemas de escalabilidade e privacidade na *blockchain*. O gerenciamento de chaves é um componente essencial em um sistema baseado em *blockchain* e cada participante de uma rede *blockchain* possui uma ou mais chaves privadas.

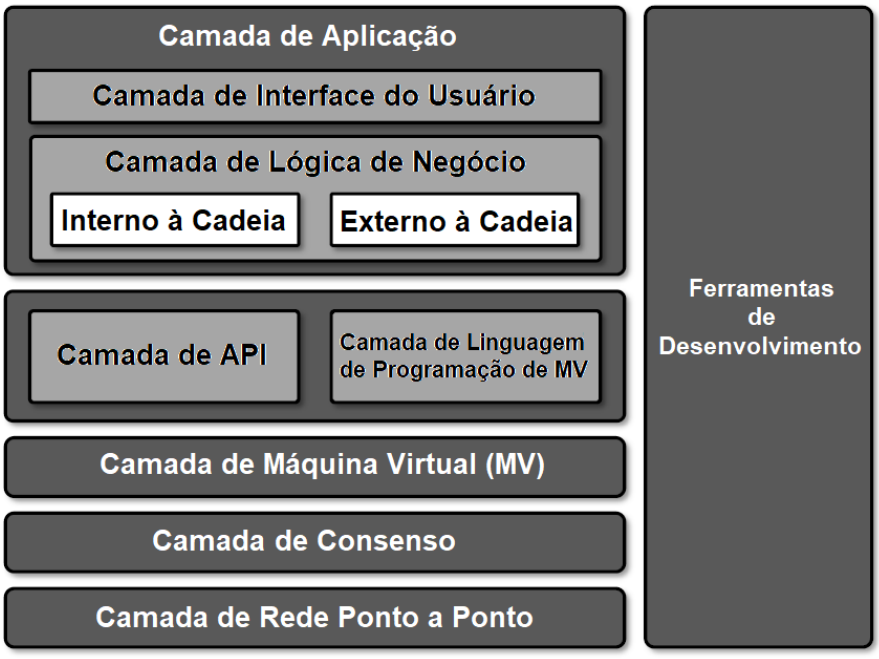
Figura 8 – *Blockchain* como um componente de sistemas de aplicativos de software



Fonte: adaptado de (LU *et al.*, 2018).

A Figura 9 exibe uma arquitetura de referência derivada por Wan *et al.* (2019), em cinco camadas de recursos. A camada de rede ponto a ponto é responsável pela comunicação entre nós. A camada de consenso fornece implementações para gerar a ordem de criação de blocos e validar blocos criados por outros nós na rede. A camada de máquina virtual é responsável pelas mudanças no estado global de uma *blockchain*. A camada de arquitetura consiste em duas subcamadas: a camada API, usada por aplicativos de *blockchain* em tempo de execução, e camada de linguagem de programação da Máquina Virtual (MV), usada no tempo de desenvolvimento e compilada em código de máquina virtual que pode ser implantado em um *blockchain* e executado pela camada de máquina virtual. A camada de aplicação consiste em duas subcamadas: camada de lógica de negócios e camada de interface do usuário. A camada de lógica de negócios fornece funcionalidades específicas do aplicativo usando o *blockchain* subjacente para fornecer soluções de negócios. Os contratos inteligentes residem na camada de lógica de negócios. A camada de lógica de negócios consiste em partes *On-chain* e *Off-chain*. A parte *On-chain* é o contrato inteligente real que geralmente é escrito em alguma linguagem de programação da MV, e a parte fora da cadeia (*Off-chain*) liga a lógica de negócios do contrato inteligente ao mundo externo.

Figura 9 – Arquitetura de referência de plataformas de *blockchain*



Fonte: adaptado de (WAN *et al.*, 2019).

2.6 Principais Aplicações da *Blockchain*

A tecnologia *blockchain* foi originalmente usada para a moeda digital Bitcoin, mas atualmente essa tecnologia está sendo implementada em muitas outras plataformas e usada para muitos outros propósitos (XU *et al.*, 2019). O potencial dessa tecnologia é imenso, sendo que aplicações estão surgindo em inúmeros setores além da própria computação (protocolos de redes, nuvem e IoT), como por exemplo, nas áreas de finanças, saúde, artes e governo (GREVE *et al.*, 2018). A realização de investimentos para desenvolvimento ou monitoramento de aplicações baseadas em *blockchain* por parte de governos em todo o mundo tem ganhado destaque. Como exemplo, existem os seguintes projetos:

- Estados Unidos da América: o governo desse país tem interesse na aplicação de *blockchain* para vários fins. Em uma das primeiras concessões de contrato para implementação da tecnologia *blockchain* para o governo dos Estados Unidos, foi uma aplicação em tempo real para dispositivos interativos portáteis para permitir a troca de dados de pacientes dentro da rede do Grupo de Trilhas de Doenças Críticas e Lesões dos Estados Unidos. Os Comandos de Transporte do Departamento de Defesa e Material e Pesquisa Médica do Exército dos Estado Unidos também demonstraram interesse nessa tecnologia (DELAHUNTY, 2018).
- Europa: o Parlamento Europeu votou a favor da adoção de uma abordagem para regular a tecnologia *blockchain*. A iniciativa do Parlamento da União Europeia (UE) combina a iniciativa da criação de uma Força-Tarefa de Moeda Virtual e a inclusão do câmbio da moeda virtual no âmbito da Diretiva Europeia Anti-Lavagem de Dinheiro. Isso tem o objetivo de evitar sufocar essa inovação tecnológica. Essa Comissão da UE foi instada para monitorar ativamente como a tecnologia evolui e oferece propostas oportunas de regulamentação específica quando necessário (YEOH, 2017).
- Chile: o governo do Chile anunciou em 2018 a utilização da tecnologia *blockchain* para registrar dados e estatísticas no setor de energia. O objetivo foi aumentar segurança, integridade, rastreabilidade e confiança da informação disponibilizada nesta área (ZOGBI, 2018).
- Brasil: o órgão de Serviço Federal de Processamento de Dados (Serpro) do governo brasileiro anunciou em 2019 uma solução que utiliza a tecnologia *blockchain* para garantir a autenticidade das informações compartilhadas entre o Brasil e países do Mercosul. Essa solução permite o compartilhamento de informações cadastrais das empresas certificadas pela Receita Federal para facilitação dos procedimentos aduaneiros, tanto no Brasil quanto

no exterior (SERPRO, 2019).

Com o advento da *blockchain*, o conceito de contratos inteligentes ganhou destaque, no qual se tornou uma área ativa de pesquisa ligada diretamente com blockchain. Devido aos benefícios de redução de custos que os contratos inteligentes podem trazer para o setor de serviços financeiros, reduzindo o custo das transações e simplificando contratos complexos, pesquisas rigorosas estão sendo realizadas por várias instituições financeiras e acadêmicas a fim de formalizar e realizar a implementação de contratos inteligentes de modo fácil e prático (BASHIR, 2017).

Existem várias aplicações possíveis nas quais contratos inteligentes podem ser aplicados. Uma delas, a área de IoT, em que existem bilhões de nós que estão compartilhando dados entre si através da *Internet*. Um caso de uso em potencial de contratos inteligentes baseados em *blockchain* é permitir que esses nós compartilhem ou acessem diferentes propriedades digitais sem terceiros confiáveis. Existem várias empresas que investigam esse caso de uso. Por exemplo, a "Slock.it" é uma empresa alemã que utiliza contratos inteligentes baseados em Ethereum para alugar, vender ou compartilhar qualquer coisa (por exemplo, vender um carro) sem o envolvimento de um terceiro confiável (CHRISTIDIS; DEVETSIKIOTIS, 2016).

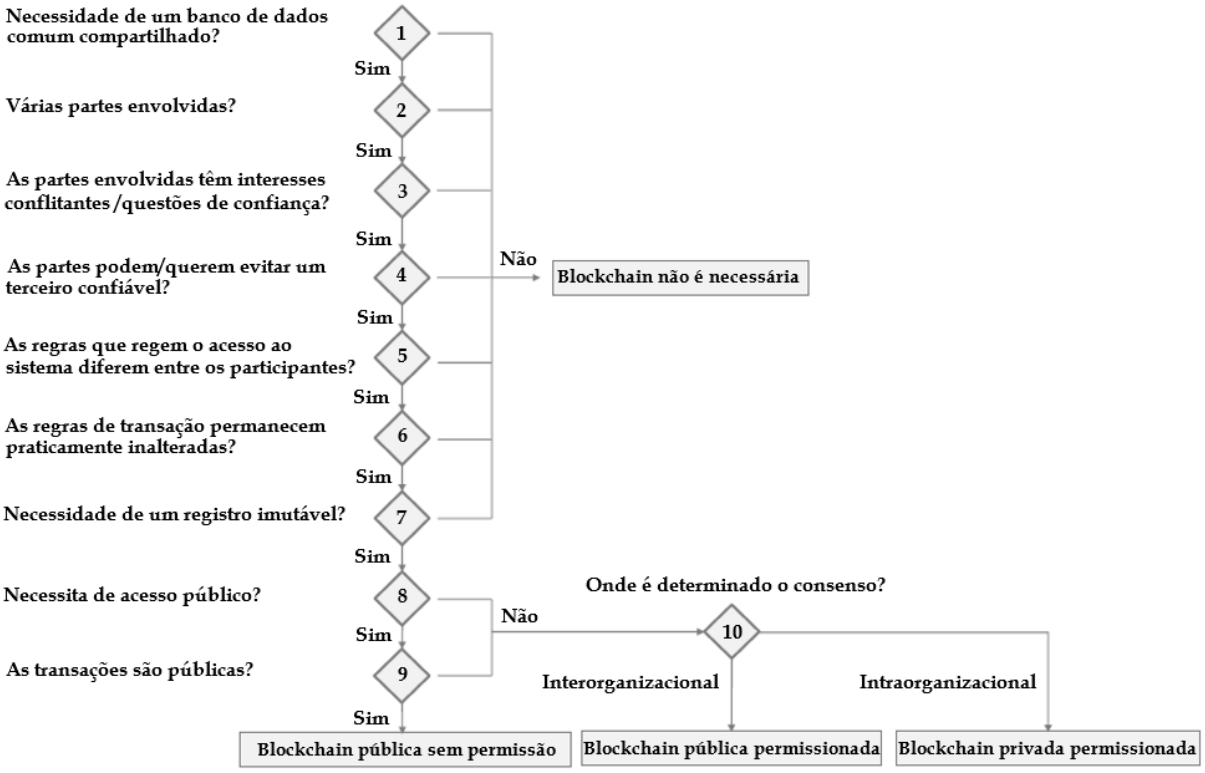
Outro caso de uso potencial é registrar os direitos de propriedade de músicas na *blockchain*. Um contrato inteligente pode impor o pagamento aos proprietários de músicas, uma vez que uma música é usada para fins comerciais. Também garante que o pagamento está sendo distribuído entre os proprietários da música. "Ujo" é uma empresa que investiga o uso de contratos inteligentes baseados em *blockchain* na indústria da música (EGBERTSEN *et al.*, 2016). O comércio eletrônico também é um caso de uso em potencial, pois poderia facilitar o comércio entre partes não confiáveis (por exemplo, vendedor e comprador), em que isso poderia resultar na redução dos custos comerciais (BANASIK *et al.*, 2016).

Existem outras aplicações possíveis, como votação eletrônica, pagamento de hipoteca, gerenciamento de direito digital, seguro de automóvel, armazenamento de arquivos distribuídos, gerenciamento de identidades e cadeia de suprimentos (ALHARBY; MOORSEL, 2017). Uma grande variedade de aplicações está surgindo rapidamente com os contratos inteligentes na *blockchain*, na qual várias organizações da indústria e academia buscam os benefícios dessa tecnologia para diversos domínios da sociedade.

2.7 Analisando Adoção da Tecnologia *Blockchain*

A *blockchain* pode acrescentar muita complexidade a qualquer área da indústria ou acadêmica, então deve-se considerar atributos de qualidade e fornecer justificativas para apoiar decisões se devem usar uma *blockchain* ou um sistema convencional. Esse é um grande desafio para arquitetos de sistemas. O trabalho de Pedersen *et al.* (2019) apresenta um caminho de decisão em dez etapas (Figura 10) que pode ajudar a determinar se a aplicação da *blockchain* é justificada. Como regra geral, o trabalho recomenda que uma *blockchain* é viável se pelo menos cinco das sete primeiras perguntas são respondidas com "Sim". Mesmo assim, os profissionais precisam equilibrar cuidadosamente vários requisitos para cada caso de aplicação de forma individual.

Figura 10 – Visão geral do caminho de decisão da *blockchain*



Fonte: adaptado de (PEDERSEN *et al.*, 2019).

Essas perguntas são discutidas com usuários experientes na lógica de negócio do ambiente analisado, permitindo uma interação mais adequada com os profissionais experientes em *blockchain* que estariam atuando na avaliação de uso dessa tecnologia. As sete primeiras questões são mais específicas sobre o uso da tecnologia *blockchain* para determinar a viabilidade da aplicação da solução. As três últimas questões ajudam a determinar qual tipo de *blockchain* seria apropriada para uma aplicação específica.

Esse passo a passo de caminho de decisão pode ser utilizado pelos profissionais para identificar se há um caso válido para adotar uma solução *blockchain*. A série de perguntas simples de sim ou não poderá ajudar os profissionais a decidir quando usar uma *blockchain* e que tipo de *blockchain* deve ser implantada. No entanto, o projeto da solução requer mais que decisões binárias, precisa levar em conta as regras de negócio mais amplas, requisitos e restrições (PEDERSEN *et al.*, 2019).

Analisando no contexto do ensino superior, contratos inteligentes em redes *blockchain* permitirão soluções para o registro e disponibilidade de certificados de forma segura e autônoma, criando transações que serão executadas somente após a conclusão de requisitos específicos. Isso não apenas permite maior automação, escalabilidade e transações mais baratas (não é necessário ter terceiros para supervisionar as transações), sendo que os contratos inteligentes também podem impedir fraudes por pessoas que desejam usar os dados em benefício próprio. As informações são compartilhadas em uma rede descentralizada e protegida por criptografia, o que dificultaria comprometer a segurança da rede (WOOD, 2019).

3 TRABALHOS RELACIONADOS

Este capítulo apresenta a estratégia de recuperação dos trabalhos relacionados a esta dissertação. Uma visão geral do assunto é apresentada para situá-lo diante da literatura obtida, assim como uma breve descrição de cada um dos trabalhos. Por fim, alguns critérios de comparação entre a proposta da dissertação e os trabalhos relacionados também são apresentados.

3.1 Planejamento da Busca por Trabalhos Relacionados

Blockchain é uma área que nos últimos anos vêm ganhando muita atenção tanto na academia quanto na indústria. Sua aplicação nas mais variadas áreas está se tornando uma realidade. Especificamente para a área educacional, *blockchain* está sendo aplicada para diversos fins, muitas vezes explorando suas características de imutabiliadde e rastreabilidade.

Baseado nas orientações descritas por Kitchenham e Brereton (2013), uma estratégia para identificação de trabalhos relacionados foi proposta.

A busca foi inspirada pela seguinte questão: "Quais trabalhos científicos utilizam *blockchain* para manipulação de certificados de alunos?". De posse dessa questão, e após o refinamento com algumas palavras chave, surgiu a seguinte *string* de busca: "*blockchain and education and diploma*".

Ao se utilizar termos como "*Higher Education*", "*undergraduation*" e "*University Degree*", os resultados eram muito limitados. Assim decidiu-se por uma *string* de busca mais genérica.

Para a busca, as seguintes bibliotecas digitais foram utilizadas: ACM Digital Library, IEEE Xplore Digital Library, Science Direct e Springer Link. Todas as palavras chave foram usadas nas fontes de pesquisa através de suas respectivas funcionalidades de busca avançada.

Como critérios de inclusão considerou-se apenas artigos científicos e sem limite de data de publicação, no idioma inglês, que estivessem disponíveis e que relatassem experiências do uso de *blockchain* no domínio educacional. Como critérios de exclusão, caso o artigo só comentasse da possibilidade do uso de *blockchain*, sem sua plena utilização ou modelagem, ele deveria ser excluído. Revisões sistemáticas e mapeamentos sistemáticos também foram descartados.

O processo de seleção seguiu os seguintes passos: (i) As palavras chaves são aplicadas na busca avançada das fontes de pesquisa; (ii) Para selecionar os estudos iniciais, são

lidos o resumo e título, e em seguida os critérios de inclusão e exclusão são aplicados; e (iii) Os documentos resultantes são lidos por completo e aplica-se novamente os critérios de inclusão e exclusão.

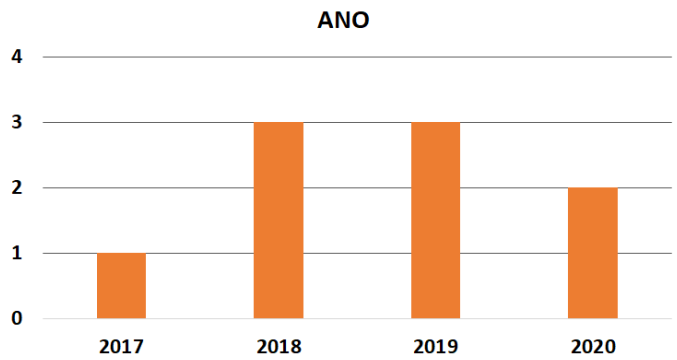
3.2 Visão Geral

O processo de extração ocorreu em setembro de 2020. Foram encontrados 15 artigos na ACM Digital Library, 7 artigos na IEEE Xplorer, 27 artigos na Science Direct e 8 artigos na Springer Link, totalizando 57 documentos. Após a aplicação dos critérios de inclusão e exclusão, resultou-se em 9 artigos, sendo 3 artigos da ACM Digital Library, 5 artigos da IEEE Xplorer e 1 artigo da Science Direct. A Springer Link não teve nenhum trabalho que se encaixasse nos critérios de inclusão.

Todos os nove trabalhos identificados na etapa final foram lidos e descritos brevemente. Algumas informações de diversos aspectos foram coletadas, dispostas e analisadas a seguir. Essas informações foram: ano da publicação, palavras chave do trabalho, trabalhos futuros, país da instituição dos autores, veículo de publicação, se desenvolveu uma aplicação, funcionalidades da aplicação, se aplicou em alguma instituição, se propôs arquitetura, se modelou a aplicação, se realizou alguma análise de desempenho e métricas para análise. Adicionalmente, as ferramentas relacionadas ao desenvolvimento com *blockchain* presentes nos trabalhos também foram coletadas. Algumas informações foram tabuladas e outras geradas gráficos.

A Figura 11 apresenta a quantidade de trabalhos identificados na busca final por ano. Apesar dos anos 2018 e 2019 possuírem cada um 3 trabalhos, e 2020 apenas 2, a tendência é que aumente esse número, pois ainda há o restante do ano com possibilidade de publicações. E como a área está começando a evoluir, também espera-se mais publicações.

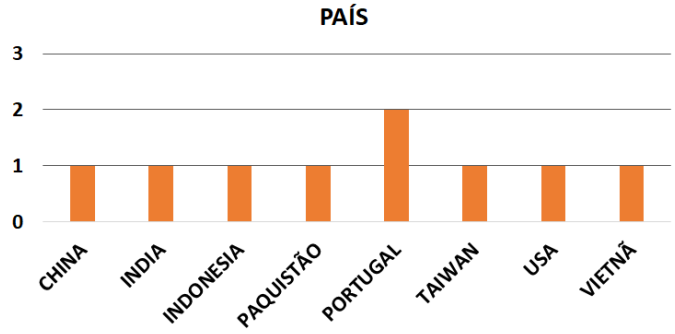
Figura 11 – Quantidade de trabalhos por ano



Fonte: o autor.

A Figura 12 apresenta a quantidade de trabalhos identificados por país. Devido ao contexto específico de educação, de 9 trabalhos, apenas dois pertenceram a um mesmo país (Portugal). Todos os demais foram de países diferentes.

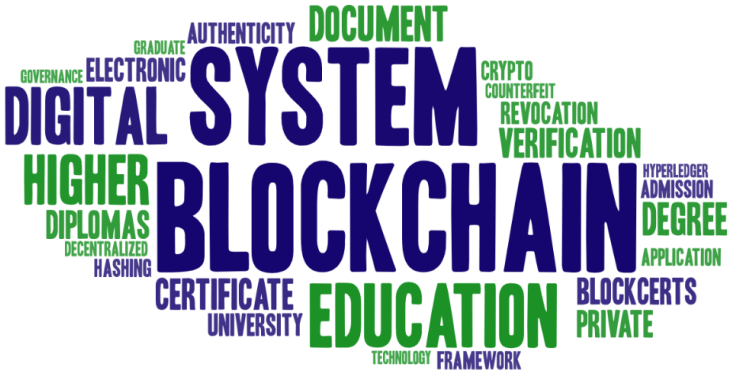
Figura 12 – Quantidade de trabalhos por país



Fonte: o autor.

A Figura 13 exibe uma nuvem de palavras construída com todas as palavras chaves definidas nos trabalhos. Com destaque para *blockchain*, sistema, educação e digital. Elementos de tecnologia também foram mencionados e funcionalidades da aplicação.

Figura 13 – Nuvem de palavras construída pelas palavras chave dos trabalhos



Fonte: o autor.

O Quadro 1 lista os veículos de publicação identificados. Apenas o primeiro está publicado em periódico, mesmo sendo uma edição originada de uma conferência. Todos os eventos foram diferentes.

3.3 Descrição dos Trabalhos Relacionados e Comparação

Para automatizar e melhorar um sistema existente na instituição, Bedi *et al.* (2020) propuseram um esquema de contrato inteligente baseado em *blockchain* para estudantes univer-

Quadro 1 – Lista de veículos de publicação identificados na pesquisa

Procedia Computer Science, International Conference on Computing and Network Communications (CoCoNet)
Annual SIG Conference on Information Technology Education (SIGITE)
International Conference on Future Networks and Distributed Systems (ICFNDS)
International Symposium on Information and Communication Technology (SoICT)
International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)
International Conference on Applied System Innovation (ICASI)
International Conference on Parallel and Distributed Systems (ICPADS)
Iberian Conference on Information Systems and Technologies (CISTI)
International Conference on Information Management and Technology (ICIMTech)

Fonte: elaborado pelo autor.

sitários. O contrato inteligente automatizaria o sistema existente, reduzindo a necessidade de trabalho manual, e consequentemente o consumo de tempo. A aplicação possui quatro entidades envolvidas: Conselho de Educação, Estudantes, Faculdades e Bancos. Uma aplicação web foi projetada e juntamente com os contratos inteligentes foram avaliadas diante de ataques de segurança.

Han *et al.* (2018) apresentaram uma técnica baseada em *blockchain* para criar um ambiente onde indivíduos possam ser os guardiões de seus registros oficiais de educação e facilmente compartilhar esses registros com outras pessoas. A solução permite que os provedores de educação emitam certificados oficiais fornecendo prova de conclusão ou realização. Esses certificados podem ser coletados por indivíduos e compartilhados diretamente com qualquer pessoa que necessite de documentos oficiais. Assim, a organização participante e o indivíduo estabeleçam um acesso autorizado aos dados pertencentes às partes correspondentes. Discutiu-se que em termos de custo, o custo do armazenamento baseado em *blockchain* pode ser metade do armazenamento baseado em nuvem típico.

Ghaffar e Hussain (2019) descreveram um sistema baseado em *blockchain* para validar e verificar graus e certificados. O sistema proposto pode verificar e validar o histórico educacional do aluno das respectivas partes interessadas educacionais. Ele permite que os alunos se inscrevam para admissão em universidades usando uma plataforma única. Usando *blockchain*, este sistema é seguro, resistente à violação, economiza tempo, é eficiente e confiável. Este trabalho é uma proposta de desenvolvimento de uma aplicação.

Nguyen *et al.* (2018) propuseram uma abordagem que utiliza a tecnologia *blockchain* para emitir certificados digitais imutáveis e melhorar as limitações atuais dos sistemas de verificação de certificados existentes, como velocidade, confiabilidade e independência da autoridade central. Para isso, foi desenvolvido um protótipo com contratos inteligentes. A implantação piloto bem-sucedida indica que a solução é aplicável a ampla implantação como um

serviço de gerenciamento de certificados e diplomas.

Vidal *et al.* (2019) descreveram uma abordagem utilizando *blockchain* implementada na Universidade Fernando Pessoa, assim como novos desafios em segurança e implementação levantados pelo uso desta tecnologia. A adoção de uma solução baseada em *blockchain* foi proposta, nomeada Blockcerts, para armazenar informação de diploma, possibilitando que qualquer pessoa verifique e visualize suas informações. Um protótipo foi implementado e discutiu-se as implicações da tecnologia e dos processos de negócios subjacentes. Neste trabalho foi sinalizado que a revogação de diplomas é um desafio.

Cheng *et al.* (2018) desenvolveram um aplicativo descentralizado e projetaram um sistema de certificação baseado na *blockchain* Ethereum, para lidar com o problema da falsificação de certificados. Pela propriedade inalterável do *blockchain*, o certificado digital com anti-falsificação e verificabilidade pode ser emitido. O procedimento de emissão do certificado digital neste sistema é o seguinte: geração do arquivo eletrônico de um certificado em papel que acompanha outros dados relacionados no banco de dados, cálculo do arquivo eletrônico para seu valor *hash*, e armazenamento do valor do *hash* no bloco do sistema de cadeia. O sistema cria um código QR relacionado e um código de sequência de consulta para afixar no certificado em papel. Também é possível verificar a autenticidade do certificado em papel por meio de digitalização em telefone celular ou consultas no site. O sistema não apenas aumenta a credibilidade de vários certificados em papel, mas também reduz eletronicamente os riscos de perda de vários tipos de certificados.

Duan *et al.* (2017) propuseram uma solução educacional com *blockchain* baseada no índice de exigência de graduação de uma universidade, com certificação profissional e que utiliza um software de avaliação automatizada como ferramenta. Para isto, uma estrutura de armazenamento na *blockchain* foi descrita, assim como a aplicação. Alguns registros de históricos de alunos foram armazenados na ferramenta, com informações de notas, cursos, indicadores, e possibilitando a geração de micro diplomas.

Ao contrário da imutabilidade, que é característica de uma *blockchain*, as operações corretivas devem ser feitas sem alterar os dados existentes e garantindo a privacidade. Tais condições tornam esta tarefa mais complexa para este tipo de sistema. Vidal *et al.* (2020) discutiram uma abordagem para tratar esse problema, sendo aplicada em um domínio real. Um aplicativo na área de ensino superior foi proposto, utilizando *blockchain* para a emissão de certificados acadêmicos e contendo um mecanismo de revogação de diplomas digitais que possam

ter sido emitidos incorretamente, por meio de contratos inteligentes. A proposta armazena as informações de revogação em um arquivo distribuído sendo compatível com qualquer *blockchain*. Também evita restrições de limitação de armazenamento.

Taufiq *et al.* (2019) apresentaram uma solução para o armazenamento de documentos de graduação em cripto-governança e prevenção de fraude de diplomas e transcrições. A seguinte questão de pesquisa foi analisada: como manter o armazenamento de documentos de graduação seguro e como ele poderia ter garantida a autenticidade? Utilizou-se como modelo os dados de alunos de uma universidade. As etapas de pesquisa foram discussão e revisão da literatura, análise, aprendizagem da tecnologia de *blockchain* e criação de um modelo do sistema. Não foi implementada uma aplicação. Espera-se com esse trabalho que os dados dos alunos de graduação possam ser encontrados de forma mais rápida, fácil e com garantia de autenticidade.

As Tabelas 1 e 2 exibem um sumário dos critérios de comparação entre os trabalhos relacionados e a proposta. Os critérios foram: (i) Desenvolveu uma aplicação?; (ii) Modelou a aplicação?; (iii) Quais funcionalidades a aplicação possui?; (iv) Aplicou em alguma instituição?; (v) Propôs arquitetura?; (vi) Que ferramenta de blockchain foi utilizada?; (vii) Executou alguma análise de desempenho?; e (viii) Quais métricas utilizou?.

Quanto à criação / desenvolvimento de uma aplicação que utilize recursos da *blockchain* para a manipulação de certificados, 7 trabalhos desenvolveram aplicações e 2 não. Outro aspecto é se modelou a aplicação. Nem todos descreveram modelos, ou não se sabe se foi modelada uma aplicação. Entende-se por essa atividade requisitos funcionais, diagramas de sequência, classes ou atividades, fluxogramas ou equivalentes. Apenas 6 trabalhos modelaram a aplicação e 3 não.

Em relação às funcionalidades que são diretamente relacionadas com *blockchain*, estas podem ter sido desenvolvidas na aplicação ou propostas no trabalho. As seguintes funcionalidades foram consideradas: inclusão do certificado na *blockchain*, validação de certificado na *blockchain*, consulta de dados do certificado à *blockchain* e revogação do certificado na *blockchain*. 9 trabalhos realizaram ou propuseram inclusões, consultas e validações. A atualização de dados também foi mencionada, mas como o estado não pode ser alterado, para isto se realiza uma nova inclusão. Apenas 2 trabalhos mencionaram revogação, sendo que um foi como um desafio e outro apenas modelou.

A aplicação em instituições, seja em produção, ou com protótipos, não foi executada por todos os trabalhos. Considerou-se também com aplicação em instituição se utilizou dados

reais para testes. 6 trabalhos aplicaram e apenas 3 não.

Tabela 1 – Comparação entre trabalhos relacionados (I = incluir, V = validar, C = consultar, R = revogar)

Artigo	Criou aplicação	Modelou aplicação	Funcionalidades	Aplicou em instituição
Bedi *et al.* (2020)	Sim	Sim	I, V, C	Sim
Han *et al.* (2018)	Não	Não	I, V, C	Não
Ghaffar e Hussain (2019)	Sim	Sim	I, V, C	Não
Nguyen *et al.* (2018)	Sim	Sim	I, V, C	Sim
Vidal *et al.* (2019)	Sim	Sim	I, V, C	Sim
Cheng *et al.* (2018)	Sim	Sim	I, V, C	Sim
Duan *et al.* (2017)	Sim	Não	I, V, C	Sim
Vidal *et al.* (2020)	Sim	Não	I, V, C, R	Sim
Taufiq *et al.* (2019)	Não	Sim	I, V, C	Não
Proposta	Sim	Sim	I, V, C, R	Sim

Fonte: o autor.

A proposição da arquitetura é importante pois demonstra certo nível de maturidade na solução e tecnologia. 8 trabalhos propuseram em níveis variados, sendo alguns descrevendo apenas com texto. E a maioria dos trabalhos utilizou a Ethereum, mas também com menções ao Bitcoin, Hyperledger e Blockcert.

Em relação à análise de desempenho, este aspecto não foi muito explorado nos trabalhos identificados. Os poucos que realizaram algo mais estruturado não descreveram o projeto de experimentos com detalhes, nem passos executados. E as métricas se resumiram a analisar tempo de verificação dos dados do usuário e valores financeiros. Os tempos em um ambiente de *blockchain* podem ser bastante variados e serem calculados de várias situações, como tempo de inclusão, de consulta, de validação do bloco, etc.

Os trabalhos apresentaram algumas ideias para trabalhos futuros, mas muito particulares para seus contextos. Por exemplo, investir em outros tipos de ataques contra a aplicação *blockchain* e desenvolvimento de aplicações *mobile* para as soluções propostas (BEDI *et al.*, 2020). Também novos modelos para múltiplas autoridades para assinaturas de certificação, ampliando as instituições envolvidas (GHAFFAR; HUSSAIN, 2019). Do ponto de vista de tecnologia, implementar e implantar a solução em várias plataformas de *blockchain* (NGUYEN *et al.*, 2018) e criação de arquivos de dados genéricos em um padrão universal (VIDAL *et al.*, 2020). Do ponto de vista de funcionalidades, desenvolver a revogação de documento na *blockchain* (VIDAL *et al.*, 2019). E do ponto de vista das possibilidades de aplicações dos dados na *blockchain*, conduzir avaliações de aprendizagem dos alunos com base nos registros da *blockchain* (DUAN *et al.*, 2017). Por fim, analisar mais profundamente os modelos propostos

Tabela 2 – Comparação entre trabalhos relacionados

Artigo	Propôs arquitetura	Ferramenta	Análise de Desempenho	Métricas
Bedi *et al.* (2020)	Não	Ethereum	Sim	Não
Han *et al.* (2018)	Sim	Ethereum	Não	Não
Ghaffar e Hussain (2019)	Sim	Não informado	Não	Não
Nguyen *et al.* (2018)	Sim	Ethereum	Não	Tempos, Taxas financeiras
Vidal *et al.* (2019)	Sim	Bitcoin, Blockcert	Sim	Taxas financeiras
Cheng *et al.* (2018)	Sim	Ethereum	Não	Não
Duan *et al.* (2017)	Sim	Ethereum	Sim	Quantidade de registros armazenados
Vidal *et al.* (2020)	Sim	Ethereum, Bitcoin, Blockcert	Não	Não
Taufiq *et al.* (2019)	Sim	Hyperledger Fabric	Não	Não
Proposta	Sim	Ethereum	Sim	Sim

Fonte: o autor.

(VIDAL *et al.*, 2020).

A proposta desta dissertação se propõe a atender a todos os critérios dispostos nas Tabelas 1 e 2 e utilizar a *blockchain* Ethereum. Uma arquitetura e aplicação será desenvolvida para atender às necessidades do domínio educacional. Uma avaliação da aplicação com especialistas será conduzida, e um projeto de experimento será planejado, com métricas de tempo e valores financeiros.

Em relação às arquiteturas apresentadas na Seção 2.5, uma diferença entre a arquitetura proposta neste trabalho é a união das camadas de forma mais adequada e simples, já que a ideia é propor uma arquitetura de referência mais fácil e flexível de se implementar. Existem diversas camadas / componentes em comum. Optou-se por não detalhar a camada de banco de dados convencional, entendendo-se que ela pode ser composta por qualquer tipo de banco de dados externo à *blockchain*. Além disso, o desenvolvimento do protótipo seguirá essa nova arquitetura.

4 ARQUITETURA E APLICAÇÃO EDUC-DAPP

Neste capítulo é apresentada a arquitetura proposta para avaliar uma nova abordagem para armazenar e consultar os dados de diplomas com a tecnologia *blockchain*. A Seção 4.1 apresenta um estudo preliminar sobre a viabilidade do uso da tecnologia *blockchain* por especialistas. Em seguida, a Seção 4.2 apresenta a arquitetura proposta neste trabalho. Na Seção 4.3, os requisitos da aplicação são apresentados. Por fim, a modelagem da aplicação é apresentada na Seção 4.4.

4.1 Análises Preliminares

Um estudo preliminar sobre a viabilidade e a utilidade da tecnologia *blockchain* para o domínio educacional foi planejado e executado. Para isso, dois profissionais do domínio educacional, com experiência de 10 anos nessa área em uma IES foram entrevistados para analisar a viabilidade e conhecer mais sobre o processo de registros de diplomas. Os dois entrevistados são responsáveis por todo o processo de emissão e registro dos diplomas na IES onde trabalham.

O objetivo da entrevista foi identificar justificativas para apoiar as decisões arquiteturais sobre a utilização da *blockchain*. Duas abordagens foram utilizadas: os dez passos propostos em Pedersen *et al.* (2019) e como usar a aplicação em comparação com o processo atual. Um protótipo simples foi apresentado aos especialistas.

4.1.1 Protótipo

Esta avaliação inicial trata da lógica de negócios do registro de diplomas, em que toda interação é realizada com uma interface semelhante a um sistema tradicional. Definiu-se assim o protótipo inicial da aplicação Educ-Dapp. Foi definido um cenário para que uma instituição de ensino superior privada realizasse a avaliação, que os usuários-chave participantes eram duas pessoas do setor de emissão de diplomas da instituição.

Foram repassadas as informações necessárias para os participantes da instituição acessarem a aplicação, bem como as informações básicas para utilização de suas funcionalidades. Também foi explicada de forma geral a tecnologia *blockchain* para terem conhecimento que a aplicação utiliza uma solução não tradicional.

Os dados educacionais inseridos pelas IES na *blockchain* são baseados no ato

administrativo da Portaria nº 1.095 do MEC. Todos os dados usados no cenário de avaliação são fictícios, ou seja, um cenário com dados semelhantes ao ambiente real para validar o protótipo criado. Os participantes cadastram a instituição com os dados básicos, nome e CNPJ. Após o registro bem sucedido, os usuários logavam na aplicação para iniciar o processo de registro do diploma.

Para registrar (efetuar o cadastro na aplicação) as informações dos diplomas de alguns alunos e também realizar a consulta de validação dos dados do diploma, foram definidos pelos participantes 10 casos (número considerado suficiente pelos participantes) de testes para compreensão do dinamismo da aplicação.

4.1.2 Etapas para Avaliação da Blockchain

Para esta análise, foi utilizado o caminho de dez etapas para determinar se o uso da tecnologia *blockchain* é justificada na aplicação desejada (PEDERSEN *et al.*, 2019). As dez etapas consistem em perguntas que devem ser feitas antes de implementar a *blockchain* para verificar se o uso da tecnologia é viável. A Figura 10 apresenta os dez passos.

Apenas as questões 1, 2, 3, 4 e 7 foram aplicadas aos especialistas em educação. Essas questões estão mais relacionadas à lógica de negócios, e as demais são técnicas e os participantes das entrevistas teriam dificuldade ou não saberiam responder. Como regra geral, Pedersen *et al.* (2019) recomenda que uma *blockchain* seja viável se cinco questões forem respondidas como "Sim". Mesmo assim, os profissionais precisam equilibrar cuidadosamente os vários requisitos para cada caso de aplicação individualmente.

Necessidade de um banco de dados comum compartilhado? *Justificativa: atualmente o registro é feito no DOU, considerada uma base de dados central do governo brasileiro.* Sim. Tendo em vista que cada instituição/empresa tem a necessidade de validar os dados dos diplomas, nada mais adequado do que uma base única e compartilhada;

Existem várias partes envolvidas? *Justificativa: quanto mais indivíduos e instituições envolvidas mais complexo é o gerenciamento da informação.* Sim. Secretaria Acadêmica, Registro de Diploma, Aluno, Empresas, Órgãos Públicos.

As partes envolvidas possuem interesses conflitantes / questões de confiança? *Justificativa: como cada instituição e o próprio governo possuem seus próprios bancos de dados mantendo cópias das informações, isso pode levar a conflitos de informações.* Sim. Há a necessidade de validação de autenticidade dos dados, tanto por parte das entidades registradoras como por parte

de quem consulta essas informações (aluno, empresas e órgãos públicos). Por existirem várias entidades envolvidas no processo, pode haver conflitos de confiança, por não serem conhecidas. Com isso, a *blockchain* pode fornecer uma formalidade para executar transações e armazenar dados.

As partes podem / querem evitar um terceiro confiável? *Justificativa: atualmente a maioria das instituições usam sistemas terceirizados para validar as informações.* Sim. Depois de validada a informação, não há necessidade de passar por terceiros (possuir sistema de outra empresa). Terceiros envolvidos no processo de validação podem prejudicar o controle e o acesso às informações dos diplomas. Com o *blockchain*, não seria mais necessário depender de sistemas de terceiros.

Necessidade de um registro imutável? *Justificativa: as bases de dados convencionais estão sujeitas a possíveis violações de segurança conhecidas na literatura.* Sim. É bom manter um registro das operações, seja consultando ou publicando esses dados. As possíveis auditorias tornam-se mais simples por meio de registros imutáveis. Os dados salvos no *blockchain* são imutáveis, o que fornece um mecanismo para auditorias futuras.

4.1.3 Avaliação de Uso Comparada ao Processo Atual

Para avaliar também o uso da aplicação Educ-Dapp comparado ao processo atual exigido pela portaria de número 1.095 do MEC, foi elaborado um questionário para uma entrevista, em que os participantes responderam de acordo com a experiência de uso da aplicação e as informações repassadas no início da avaliação. As respostas foram mescladas para apresentar a conclusão de cada indagação.

Qual o nível dificuldade em usar o sistema Educ-Dapp comparado ao processo atual? *Justificativa: é interessante avaliar o nível de dificuldade entre o sistema Educ-Dapp e o processo atual.* Comparado ao processo atual, a Educ-Dapp parece mais simplificada, pois para registrar os diplomas no DOU existe um formato e uma configuração específica. Além do registro no DOU também é necessário configurar os diplomas em um sistema terceirizado que temos, pois ele é o responsável pela função de consulta externa.

Você acha que a ideia da Educ-Dapp ajuda a melhorar o processo de registro de diplomas? *Justificativa: é interessante avaliar as vantagens da aplicação para o processo interno da instituição.* Com a aplicação Educ-Dapp acreditamos que simplificaria parte do processo atual que realizamos em um sistema terceirizado.

Você acredita nos benefícios apontados pela tecnologia *blockchain* que é a base da solução proposta? *Justificativa: é interessante avaliar o nível de confiança que essa nova tecnologia repassa para os participantes da avaliação.* Como se trata de uma tecnologia nova, não sabemos informar se os benefícios ocorrem realmente na prática.

Existe alguma sugestão de melhoria? *Justificativa: é interessante avaliar se os participantes veem as limitações da tecnologia blockchain.* Essa questão de criar uma carteira de *criptomoeda* no *plugin* MetaMask para pagar pelas transações é difícil de alinhar com os processos internos de pagamentos que temos na instituição, ou seja, não sabemos como tratar esse custo financeiro dentro da nossa contabilidade. Essa é uma questão legal que deve ser analisada antes de usar esse tipo de solução no mercado.

As respostas ao questionário apontam para vantagens no uso do modelo proposto, mas as instituições e os formuladores de políticas devem considerar os desafios relacionados à segurança, privacidade, custo, escalabilidade e disponibilidade antes de adotar a tecnologia *blockchain*.

4.2 Arquitetura

Arquiteturas de referência surgiram como um tipo especial de arquitetura de software que alcança uma compreensão bem reconhecida de domínios específicos, promovendo a reutilização da experiência em projeto, facilitando o desenvolvimento, padronização e evolução dos sistemas de software (NAKAGAWA *et al.*, 2012)(NAKAGAWA *et al.*, 2014).

Nesse contexto, o ProSA-RA (NAKAGAWA *et al.*, 2014) é um processo que sistematiza o projeto, a representação e a avaliação de arquiteturas de referência. Ele possui as seguintes etapas: (i) Investigação da Fonte de Informação, (ii) Análise de Arquitetura, (iii) Síntese Arquitetural, e (iv) Avaliação Arquitetural.

Na primeira etapa, as principais fontes de informação são selecionadas. Essas fontes devem fornecer informações sobre processos e atividades que podem ser suportados por sistemas de software do domínio de destino. Como as arquiteturas de referência devem ser a base de vários sistemas de software de um determinado domínio, essas fontes devem envolver um conhecimento mais abrangente sobre o domínio se comparadas às fontes de informação no desenvolvimento da arquitetura de um sistema específico.

Na segunda etapa, baseado nas fontes selecionadas, três conjuntos de elementos são identificados. Primeiramente é identificado o conjunto de requisitos dos sistemas de software

desse domínio. Com base nesses requisitos, o conjunto de requisitos da arquitetura de referência é então identificado. Por fim, é estabelecido o conjunto de conceitos que devem ser considerados na arquitetura de referência.

Na terceira etapa, a descrição arquitetural da arquitetura de referência é construída usando RAModel como uma estrutura geral. O RAModel (*Reference Architecture Model*) é um modelo de referência para arquiteturas de referência, que apresenta possivelmente todos os elementos que podem estar contidos em arquiteturas de referência, organizados por tipos e relacionamentos (NAKAGAWA *et al.*, 2012). Por exemplo, estilos e padrões arquiteturais, bem como uma combinação desses e de outros estilos, devem ser considerados. Esses estilos e padrões são a base sobre a qual os conceitos previamente identificados são organizados.

Na quarta etapa, a avaliação da arquitetura é conduzida. Por avaliação de referência refere-se à tarefa de verificar a descrição da arquitetura dessa arquitetura em conjunto com as diversas partes interessadas, com o objetivo de detectar defeitos nesta descrição. Para isso, o ProSA-RA utiliza uma abordagem de inspeção baseada em *checklist*. Em resumo, o *checklist* corresponde a uma lista de questões que orientam os revisores na detecção de defeitos em documentos relacionados a arquiteturas de referência.

Neste trabalho, os passos descritos no ProSA-RA (NAKAGAWA *et al.*, 2014) foram utilizados como base de inspiração para a elaboração da arquitetura de referência. Para isso, as fontes de informação relacionadas ao domínio educacional e os requisitos do sistema foram identificados, algumas visões arquiteturais foram modeladas, e para a avaliação, utilizou-se um questionário *online* aplicado aos especialistas.

A *blockchain* pode ser visualizada como um componente de software para ajudar a entender os impactos arquitetônicos no desempenho e na qualidade de atributos como segurança, privacidade e escalabilidade. Como um componente, a *blockchain* possui propriedades e limitações únicas e complexas, baseados em rede e que podem fornecer armazenamento de dados, serviços de computação e comunicação (XU *et al.*, 2019). A arquitetura de referência proposta neste trabalho foi baseada em Lu *et al.* (2018), Wan *et al.* (2019), Xu *et al.* (2018), Xu *et al.* (2019). Seus elementos estão descritos a seguir:

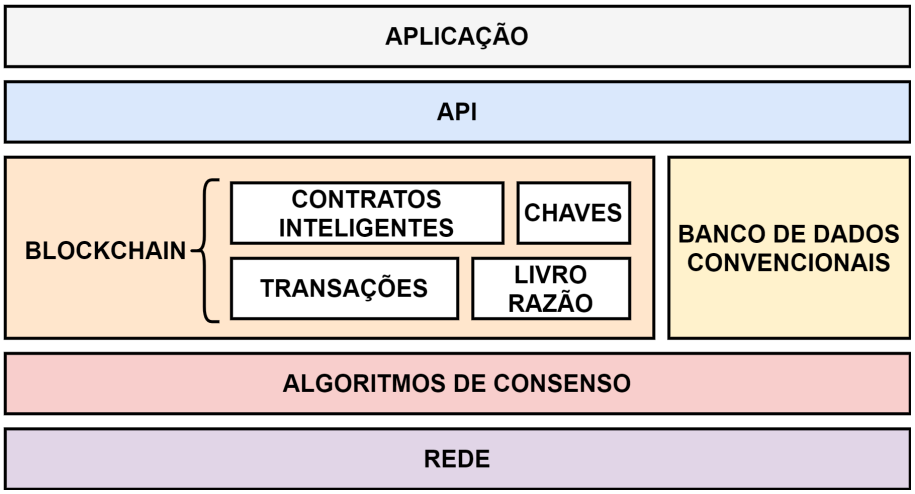
- **Aplicação:** Esta camada inclui aplicações que usam recursos de uma *blockchain*. Essas aplicações podem incluir lógica de negócios e dados, além de ter uma interface gráfica do usuário;
- **API:** A *blockchain* pode interagir com elementos do mundo externo. Esta comunicação é

feita através de APIs, tanto para consulta como para inserção de dados;

- **Blockchain:** A camada de *blockchain* é responsável por armazenar e compartilhar dados, além de executar contratos inteligentes. Está subdividida nos seguintes componentes: (i) Contratos inteligentes: Um contrato inteligente é um programa criado pelo usuário, implantado e executado na *blockchain* e pode representar regras de negócios. Eles também podem ser implementados como parte de uma transação; (ii) Transações: Este componente possui implementações para a geração e validação dos blocos e seu pedido; (iii) Chaves: o componente para gerenciamento de chaves permite que os participantes da *blockchain* possuam suas chaves privadas, usadas para assinar transações digitalmente; (iv) Livro-razão: Componente que representa o livro-razão (livro de registros) distribuído na *blockchain*;
- **Banco de dados convencionais:** Bancos de dados para auxiliar no armazenamento de dados que não serão armazenados na *blockchain*, seja pelo tamanho grande, seja por escalabilidade ou privacidade;
- **Algoritmos de consenso:** Esta camada permite implementações para gerar a ordem dos blocos e validações pelos nós da rede, com algoritmos definidos; e
- **Rede:** Camada responsável pela comunicação entre os nós, incluindo descoberta, propagação de transações e blocos.

A Figura 14 apresenta a arquitetura de referência de *blockchain* proposta, bem como suas camadas e componentes, que é a base para a criação da arquitetura proposta.

Figura 14 – Arquitetura de referência de *blockchain* proposta



Fonte: o autor.

A arquitetura de *blockchain* proposta é diferente das arquiteturas usuais em alguns aspectos. A maneira como a solução é construída e mantida é diferente das formas tradicionais.

A aplicação executa as transações utilizando um algoritmo de *hash* ou prova de trabalho para computar as informações por meio de um processo de consenso em uma rede com vários nós, garantindo a integridade das informações armazenadas na *blockchain*. Este é um processo complexo, mas atualmente existem várias ferramentas que encapsulam toda esta complexidade, facilitando a criação e manutenção deste tipo de aplicação. Com isso, é possível ter um sistema com segurança, armazenamento, alta disponibilidade e controle de acesso.

Ao construir a abordagem baseada em *blockchain*, percebe-se que existem vários componentes específicos da área de *blockchain*. Com isso, foi necessário propor e utilizar um novo modelo arquitetônico como referência. Conforme definido em Xu *et al.* (2019), com esta arquitetura de referência, informações sobre o mundo fora da *blockchain* podem ser fornecidas por aplicações específicas, em que normalmente adicionam essas informações à *blockchain* por meio de transações. O gerenciamento de chaves permite o controle de acessos a uma *blockchain*.

Parte de uma aplicação pode ser implementada no componente *blockchain* usando contratos inteligentes. *Blockchains* podem ser usados como componentes de software, que podem fornecer armazenamento de dados, serviços de computação, serviços de comunicação e funções de gerenciamento. Para sistemas baseados em *blockchain*, uma das principais decisões arquiteturais são sobre quais partes dos dados devem ser incluídos ou não na cadeia de dados. No entanto, a quantidade de poder computacional e espaço de armazenamento de dados em uma *blockchain* podem ser limitados. Assim, partes de uma aplicação implementada fora do componente *blockchain* podem hospedar dados *offline* e lógica da aplicação (XU *et al.*, 2019).

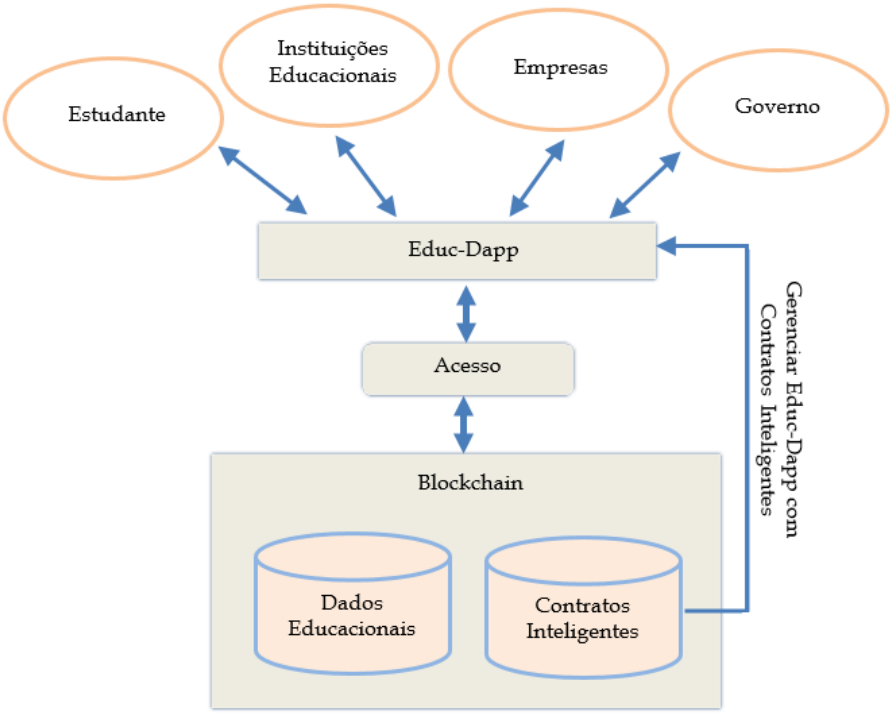
A arquitetura proposta neste trabalho visa fornecer um ambiente confiável e seguro por meio da *blockchain* para publicação de extratos de informações de certificados de alunos do ensino superior, bem como a consulta para validação de dados dos certificados. Com essa tecnologia, é possível reduzir os riscos de perda de informações e, por meio do princípio da verificabilidade dos dados, evitar a falsificação de certificados.

A Figura 15 apresenta a arquitetura proposta dividida em três camadas: (i) camada de aplicação, exemplificada pela aplicação Educ-Dapp, responsável por interagir com entidades externas ao sistema; (ii) camada API, composta pelas tecnologias necessárias para criar o acesso *blockchain*; e (iii) camada *Blockchain*, onde residem os dados educacionais e os contratos inteligentes.

Observando na arquitetura de referência (Figura 14), tem-se uma camada de algoritmo de consenso, a qual oferece um conjunto de regras que estabelece como os blocos

devem ser construídos na camada de *blockchain*. A participação no processo de construção de consenso pode ser apoiada por várias estruturas diferentes: Prova de Trabalho, Prova de Participação, Tolerância a Falhas Bizantinas. Independentemente do método utilizado, os nós da rede participam ativamente desse processo de consenso. Também tem-se na arquitetura de referência a camada de rede, onde as aplicações e processos de negócios são determinados a partir de sua estrutura descentralizada. Para que a conexão com a rede seja estabelecida, um nó deve ser capaz de processar mensagens específicas dessa rede e afetar seu estado. Essas camadas de consenso e algoritmo de rede estão incorporadas à lógica da arquitetura proposta, sendo camadas muito focadas em infraestrutura e redes, portanto não são o escopo deste trabalho.

Figura 15 – Arquitetura proposta



Fonte: o autor.

Na arquitetura proposta, a primeira camada é composta pela aplicação descentralizada Educ-Dapp (*front-end*), responsável pela comunicação direta com entidades discentes, instituições de ensino, empresas e governo, que são as principais entidades interessadas definidas neste trabalho. As instituições educacionais e entidades governamentais (por exemplo, o MEC) são as únicas que podem inserir dados na *blockchain*. Na criação do contrato inteligente automaticamente será gerado um *login* para o governo acessar o sistema, que ficará responsável pela entrada dos dados básicos das IES, que serão o nome e cadastro nacional da pessoa jurídica (CNPJ) das instituições de ensino regulares que podem emitir certificados. Assim, esses dados

serão utilizados para validação no momento em que uma instituição de ensino estiver fazendo seu cadastro na aplicação, ou seja, ela só poderá se cadastrar se o governo tiver informado previamente seus dados básicos na aplicação. Caso contrário, indica que não tem autoridade para registrar certificados. As instituições que conseguem realizar o cadastro podem inserir os dados dos diplomas dos alunos na *blockchain*. As entidades estudante e empresa (assim como qualquer outra) podem consultar os dados dos diplomas sem a necessidade de cadastro, bastando ter o número do cadastro da pessoa física (CPF) do aluno.

A segunda camada é formada pelas tecnologias responsáveis pela integração do *front-end* da aplicação com a camada *blockchain*. Para criar uma aplicação com *blockchain* é necessário utilizar configurações específicas no *front-end* a fim de estabelecer uma comunicação com a *blockchain*, ou seja, existem ferramentas específicas para o uso dessa tecnologia. Esta camada corresponde à camada API da arquitetura de referência, fornecendo tecnologias que permitem aos desenvolvedores acessar os recursos necessários e integrá-los as aplicações criadas para interagir com a *blockchain*.

A terceira camada do ambiente é formada pela *blockchain* (*back-end*) que armazena os dados educacionais dos alunos, que serão utilizados para validação no momento da consulta por entidades externas. Essa camada também armazena o contrato inteligente, que define as regras de como os dados educacionais serão armazenados e acessados. Essas regras do contrato inteligente são configuradas na aplicação Educ-Dapp para gerenciar as solicitações de consulta e inserção dos dados educacionais na *blockchain*.

Para este trabalho, foram definidos os seguintes dados mínimos para o registro de diploma na aplicação (os dados inseridos pelas IES na *blockchain* são baseados no ato administrativo da Portaria nº 1.095 do MEC):

- Nome da instituição;
- Número do CNPJ da instituição;
- Nome do aluno de graduação;
- CPF do aluno de graduação;
- Nome e código do MEC do curso superior;
- Data de ingresso no curso;
- Data de conclusão do curso.

Para as IES foram definidos apenas os seguintes dados básicos para ser possível criar um perfil para controle de acesso na aplicação:

– Nome da instituição;
– Número do CNPJ da instituição;
– Senha para acesso a aplicação.

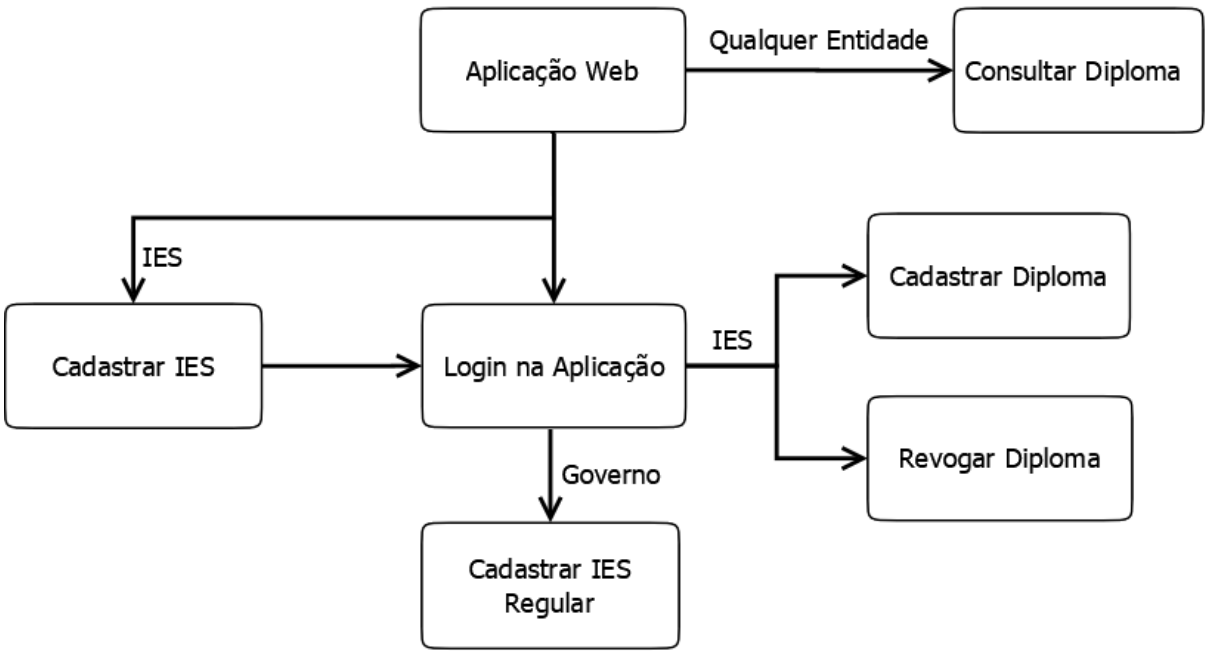
Para entidade governo, também foram definidos apenas dados básicos para criação do perfil na aplicação, sendo que o cadastro do governo é feito no momento da implantação do contrato inteligente na *blockchain*. A seguir os dados básicos:

– Nome do governo;
– Identificador;
– Senha para acesso a aplicação.

As IES realizam um cadastro na aplicação utilizando usuário (CNPJ da IES) e senha para ter direito a registrar os diplomas, sendo que a aplicação faz uma validação verificando se a mesma tem o cadastro prévio informado pelo governo. Caso sim, o sistema confirma o cadastro realizado pela instituição, ou seja, a mesma vai possuir *login* e senha para acessar a aplicação e registrar os diplomas. Dessa maneira impede que qualquer pessoa faça um cadastro na aplicação. As demais entidades possuem somente a permissão de consultar os dados dos diplomas, por meio da busca pelo CPF do estudante. O governo detém acesso a aplicação por meio do usuário (identificador) e senha criados no momento da implantação do contrato inteligente na *blockchain*.

O fluxo da aplicação proposta está apresentado no diagrama da Figura 16 para melhorar o entendimento dos recursos da aplicação.

Figura 16 – Visão geral do fluxo da aplicação proposta



Fonte: o autor.

Esse fluxo apresenta uma visão geral da aplicação independente das tecnologias utilizadas. Os detalhes de cada etapa estão descritos a seguir:

- **Aplicação Web:** Primeiramente é necessário acessar a aplicação *web*, em que por meio dela é possível utilizar as funcionalidades do ambiente proposto;
- ***Login* na Aplicação:** Tanto a entidade governo como IES conseguem realizar o *login* na aplicação, porém o acesso inicial a aplicação está autorizado somente para o governo, pois o seu perfil foi criado no momento da implantação do contrato inteligente na *blockchain*. Para as IES terem acesso, será necessário o governo realizar um cadastro prévio na aplicação informando os dados básicos (nome e CNPJ) de cada IES;
- **Cadastrar IES Regular:** O governo possui a função de cadastrar as IES que são reconhecidas, ou seja, quem pode cadastrar diplomas na aplicação. Essa é uma forma de controle para simular a interação de órgãos públicos (por exemplo, o MEC) com a aplicação.
- **Cadastrar IES:** Após o governo realizar o cadastro prévio da IES, a mesma está habilitada para realizar seu autocadastro na aplicação;
- **Cadastrar Diploma:** Após acessar a aplicação, a IES pode realizar o cadastro de diplomas;
- **Revogar Diploma:** Após acessar a aplicação a IES pode realizar a revogação de diplomas. Revogar um diploma significa corrigir o mesmo, por motivos de erros ou fraude nos dados no momento do cadastro; e
- **Consultar Diploma:** Qualquer entidade que acessar a aplicação poderá consultar os dados do diploma sem a necessidade de realizar um cadastro prévio.

Esta abordagem funciona como um novo modelo de negócio para as IES, estudantes e governo, possuindo características e formas próprias de lidar com o armazenamento e controle de acesso dos dados dos certificados dos alunos. Este modelo de negócios usa a tecnologia *blockchain* para criar um ambiente onde as IES podem armazenar informações de certificados de alunos de maneira segura e distribuída, sem a necessidade de configurar uma infraestrutura interna. Qualquer entidade externa ao sistema pode consultar o banco de dados de registros de diploma armazenados na *blockchain*. Essa abordagem aproveitará a propriedade inalterável da *blockchain* e o princípio de verificabilidade dos dados para evitar falsificação de certificados e otimizar o tempo de consulta para a veracidade dos dados.

4.3 Requisitos da Aplicação

O levantamento de requisitos para o desenvolvimento da aplicação proposta foi com base na Portaria nº 1.095 do MEC. A Educ-Dapp é uma simulação de uma possível solução *web* para qualquer entidade consultar diplomas registrados no DOU. A ideia desse trabalho não é substituir o DOU e sim criar uma solução *web* para que todos possam consultar os diplomas registrados no DOU, ou seja, cada IES continuará sendo responsável pelo o registro no DOU, em que após a confirmação dos registros, as IES podem cadastrar os diplomas na aplicação proposta. Dessa forma, a consulta aos dados dos diplomas estarão disponíveis em uma solução *Web*, conforme requisito da Portaria nº 1.095 do MEC. Os Requisitos Funcionais (RF) da aplicação estão apresentados a seguir:

- **RF1 - Cadastro de diploma:** As IES deverão manter banco de informações de registro de diplomas segundo a Portaria nº 1.095. Com isso, após o devido registro no DOU, os dados dos diplomas serão cadastrados na *blockchain* como forma de manter um banco de informações dos registros realizados DOU;
- **RF2 - Consulta do diploma:** Segundo a Portaria nº 1.095, as IES devem disponibilizar na *web* uma consulta aos diplomas, após realizado o devido registro no DOU. Essa consulta é realizada utilizando o CPF do aluno;
- **RF3 - Revogação do diploma:** Segundo a Portaria nº 1.095, as IES públicas e privadas deverão tornar nulos os atos de expedição e de registro de diplomas, quando inidôneos ou eivados de vícios de legalidade ou quando constatada falsidade documental ou declaratória. Para revogar um diploma basta informar o número de CPF do aluno;
- **RF4 - *Login* na aplicação:** Para as entidades governo e IES terem acesso as funções que inserem dados da *blockchain* é necessário realizar *login* na aplicação. No momento do *login* a aplicação deve se conectar com a extensão MetaMask ativa no navegador para assinar todas transações realizadas na aplicação. Essa extensão representa a conta da carteira de *criptomoeda* do usuário na plataforma Ethereum;
- **RF5 - Cadastro de IES regular:** A aplicação deve permitir que o governo controle quais IES podem cadastrar diplomas na aplicação. Dessa maneira, impede que uma IES irregular realize cadastros de diplomas na aplicação;
- **RF6 - Autocadastro de IES:** A aplicação deve permitir que a IES possa se cadastrar na aplicação, porém somente se o governo realizar seu cadastro prévio informando o nome e CNPJ da IES para aplicação.

Os Requisitos Não Funcionais (RNF) da aplicação estão descritos a seguir:

- **RNF1:** A aplicação deve ser compatível com os navegadores onde é possível instalar a extensão MetaMask (Chrome, Firefox, Opera e Brave);
- **RNF2:** A aplicação deve possuir *design* responsivo;
- **RNF3:** Os dados devem ser armazenados de maneira segura, podendo ser acessados apenas por entidades com autorização;
- **RNF4:** A aplicação deve fornecer um fluxo de fácil compreensão para facilitar a aprendizagem e recordação;
- **RNF5:** O ambiente da aplicação deve ser dividido em camadas para facilitar a manutenção e reduzir o acoplamento.

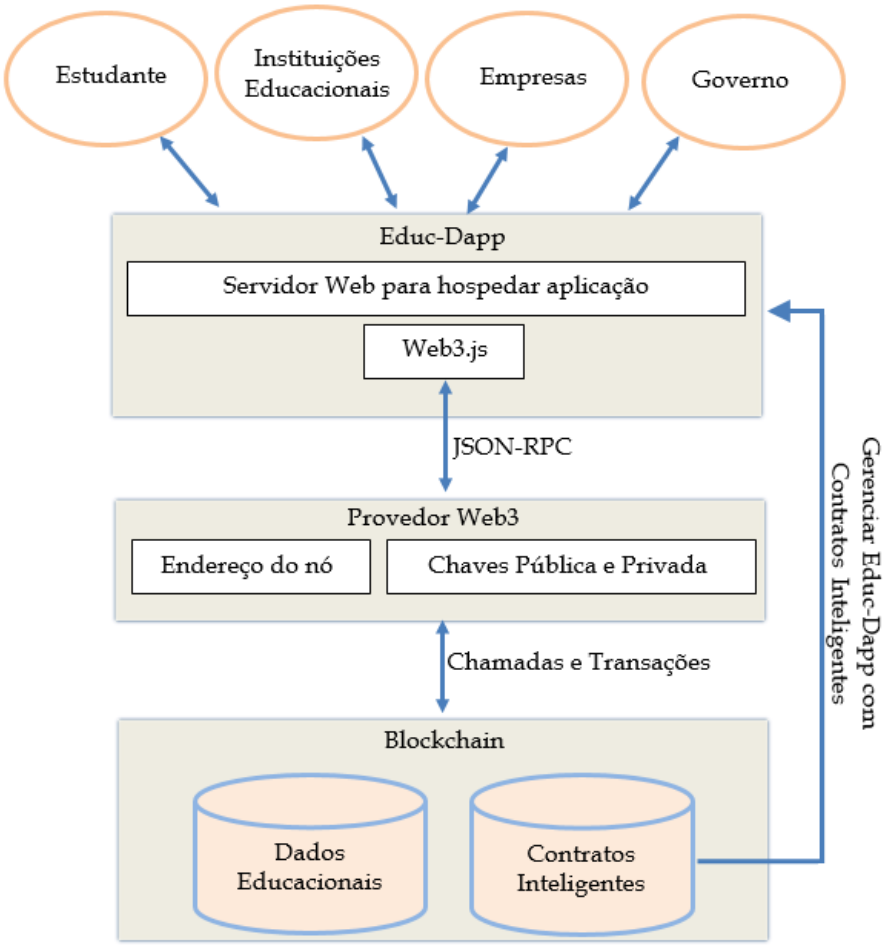
4.4 Modelagem da Aplicação

A Figura 17 apresenta uma visão ampliada da arquitetura proposta, detalhando os diversos aspectos envolvidos na modelagem. É possível visualizar os detalhes dos três principais componentes da arquitetura. A seguir serão detalhados esses componentes.

O primeiro componente é a Educ-Dapp, uma aplicação *web* desenvolvida utilizando JavaScript, HTML e CSS. Cada página *Web* da aplicação utiliza essas tecnologias para criar a interface e definir os comportamentos. Essa aplicação se comunica com os contratos inteligentes armazenados na *blockchain* através da API Web3.js, em que envia as requisições JSON-RPC (*JSON Remote Procedure Call*) para um provedor Web3 que é responsável em direcionar as transações para o nó existente dentro da *blockchain* da plataforma Ethereum. As páginas da aplicação que interagem com os contratos inteligentes são configuradas com o endereço do mesmo, o código em JSON correspondente ao código Solidity compilado e a especificação da *Application Binary Interface* (ABI) do contrato, que descreve as assinaturas dos métodos e a maneira de interagir com o contrato inteligente. Esse primeiro componente tem também um servidor *web* para hospedar a aplicação e publicar um domínio na *web* para utilizar a aplicação.

O segundo componente é o provedor Web3, em que se responsabiliza pela comunicação entre a API Web3 e a *blockchain* da plataforma Ethereum. O provedor Web3 utilizado é o MetaMask, onde é possível criar uma conta para realizar as transações na rede da Ethereum. Esse provedor recebe as requisições JSON-RPC do primeiro componente através da API, juntamente com informações sobre as chaves pública e privada para identificar a conta na *blockchain* e em seguida realizar a comunicação com o terceiro componente para submeter as transações e

Figura 17 – Visão ampliada da arquitetura proposta



Fonte: o autor.

retornar as respostas. Nesse segundo componente também é utilizado um provedor do Infura (serviço de infraestrutura para a *blockchain* da Ethereum) para criar um nó remoto da Ethereum para submeter as transações que não precisam da identificação da conta do usuário. Dessa forma, não precisa manter um nó local da *blockchain*.

O terceiro componente corresponde a *blockchain*, sendo o principal componente da arquitetura, em que armazena todas as informações da aplicação e processa as transações. A lógica de negócio e a forma de armazenar a estrutura dos dados são definidos nos contratos inteligentes implantados na *blockchain*. Existe um endereço para o contrato inteligente armazenado na *blockchain*, em que através dele é possível realizar interações como chamadas e transações com o contrato. As chamadas são funções que apenas retornam os dados, ou seja, não realizam alteração nos dados armazenados na *blockchain*. Enquanto as transações são funções do contrato que inserem ou modificam os dados na *blockchain*, tendo um custo (*gas* e *ether*) associado para conta do usuário (MetaMask) que será cobrado no momento de submeter as transações.

Transformar requisitos em código pode demandar várias iterações até a fase de

implantação do contrato inteligente. Depois de desenvolvida, a versão codificada do contrato é enviada ao livro de registros distribuídos para publicação na rede *blockchain*. A Ethereum possui a EVM que permite que os desenvolvedores criem qualquer tipo de aplicação da maneira que desejar. Os desenvolvedores instruem a EVM a executar aplicações usando uma linguagem de alto nível chamada Solidity, que é fortemente tipada, com herança e orientação a objetos (CHENG *et al.*, 2018). Os detalhes da implementação e das tecnologias utilizadas serão descritos no capítulo seguinte.

5 DESENVOLVIMENTO E AVALIAÇÃO DE DESEMPENHO DO PROTÓTIPO DA ARQUITETURA PROPOSTA UTILIZANDO CONTRATOS INTELIGENTES

Neste capítulo é apresentada a implementação de um protótipo do ambiente da arquitetura proposta utilizando contratos inteligentes baseados na plataforma Ethereum. A Seção 5.1 apresenta os detalhes da implementação e das tecnologias utilizadas. Em seguida, a Seção 5.2 apresenta os detalhes dos cenários de avaliação realizados com especialista na gestão de diplomas. Na Seção 5.3 é apresentada a análise de desempenho conduzida com base nas transações realizadas no protótipo. Por fim, as análises e discussão dos resultados obtidos na Seção 5.4 são apresentados.

5.1 Implementação da Solução Proposta

No desenvolvimento de soluções baseadas em *blockchain*, algumas tecnologias e plataformas foram analisadas. A plataforma *Ethereum* foi selecionada para o desenvolvimento deste trabalho. Nessa plataforma existe o conceito de contrato inteligente que é uma *blockchain* mais generalizada, expandindo as transações para operações computacionais que podem ser programadas para executar determinadas regras (CHRISTIDIS; DEVETSIKIOTIS, 2016).

5.1.1 Infraestrutura

Existem várias redes no mercado atualmente que podem trabalhar com a criação de contrato inteligente. Além da rede Ethereum, existem outras plataformas com propósito similar, como por exemplo: Ethereum Classic, EOSIO, Lisk, Tron, NEO, Stellar, Ripple, NEM e QTUM. A Ethereum foi selecionada para esse trabalho devido a indicação atual de utilização para execução de contrato inteligente no contexto da *blockchain* (KORPELA *et al.*, 2017). Ela possui a EVM (WOOD, 2019), onde foi criada uma aplicação (contratos inteligentes), que funciona exatamente como programado sem qualquer possibilidade de censura ou fraude, pois o contrato é imutável.

A lista a seguir descreve as tecnologias associadas a Ethereum utilizadas neste trabalho:

- **IDE Remix:** IDE *online* utilizada para desenvolvimento de contratos inteligentes;
- **Visual Studio Code:** editor de código-fonte utilizado para o desenvolvimento da interface

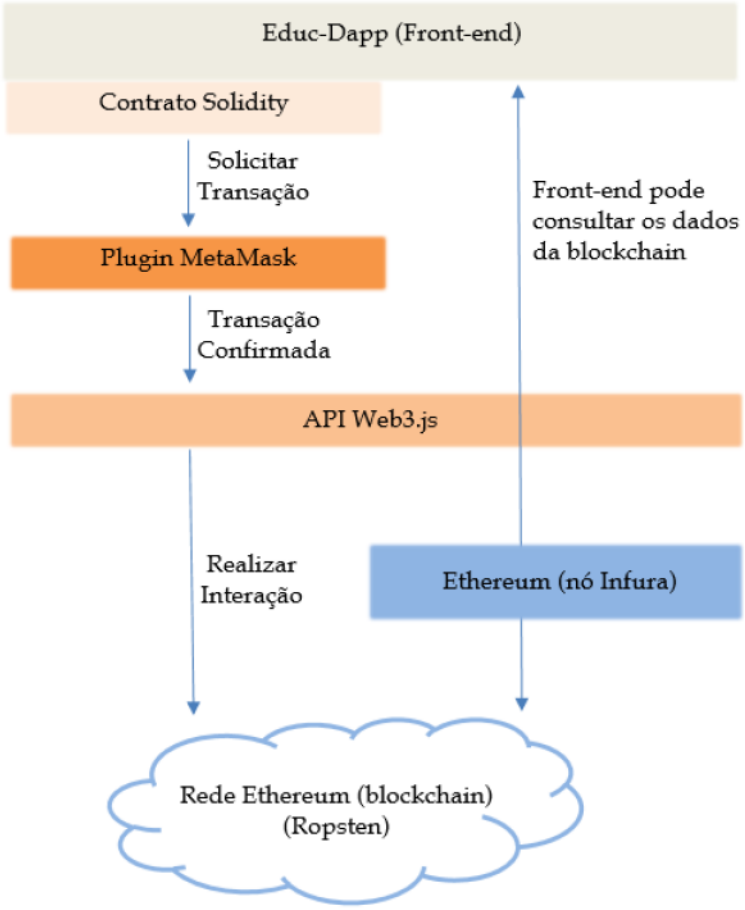
web;

- **HTML5/CSS3:** tecnologias usadas para o desenvolvimento do *front-end* da aplicação;
- **Solidity:** linguagem criada pela própria Ethereum para o desenvolvimento de contratos inteligentes;
- **API Web3.js:** documentação da Web3 JavaScript Dapp API usada para o desenvolvimento de aplicações descentralizadas;
- **Metamask:** *plugin* para o navegador (Chrome, Firefox, Opera e Brave) acessar à plataforma Ethereum, funcionando como uma carteira de *ether* e também navega na rede Ethereum sem a necessidade de ter uma cópia da *blockchain* instalada no ambiente local;
- **Ropsten:** rede pública de testes da Ethereum usada para validar a aplicação. Ela utiliza *criptomoeda* "falsa" para viabilizar testes de aplicações;
- **Infura:** serviço de infraestrutura de *blockchain* da Ethereum para interagir com o contrato inteligente criado, pois precisa-se estar conectado com um nó, que é a porta de entrada para a rede da Ethereum. O Infura possui diversos nós nas redes da *blockchain* da Ethereum, provendo uma camada de abstração para esses nós, em que a partir do endereço do projeto no Infura tem acesso a rede da Ethereum;
- **Etherscan:** ferramenta para explorar uma *blockchain*, permitindo analisar transações na plataforma Ethereum como forma de ajudar na avaliação durante o desenvolvimento da aplicação.

Na Figura 18 pode-se ter uma visão geral do fluxo de execução das tecnologias utilizadas durante as execuções de transações no protótipo criado. Na aplicação, as entidades podem usar a *blockchain* para enviar e recuperar os dados.

O objetivo do *front-end* é fornecer uma interface para o usuário interagir com o contrato inteligente criado. No *front-end* são realizadas todas as configurações necessárias para interagir com a rede da Ethereum, principalmente a descrição das assinaturas dos métodos do contrato e a maneira de interagir com ele. Para isso, o código em JSON correspondente ao código Solidity compilado e a especificação da ABI do contrato são informados no *front-end*. Quando uma solicitação é realizada a mesma só será executada após confirmação da transação pelo *plugin* MetaMask. Em caso positivo, a API Web3.js reconhece o código em Solidity que está no formato JSON e inicia a comunicação com a rede *testnet* Ropsten da Ethereum. Essa rede realiza o processo de consenso com a participação dos nós da *blockchain* para a mineração de um novo bloco para armazenar todos os dados relacionados a transação solicitada. Após esse processo

Figura 18 – Fluxo de execução das tecnologias utilizadas



Fonte: o autor.

é possível consultar os dados sem restrições de acesso diretamente na *blockchain* através do endereço do nó Infura informado no *front-end*. Com isso, para consultar os dados existentes na *blockchain* não é necessário utilizar o *plugin* MetaMask, pois após os dados inseridos na blockchain, qualquer entidade pode consultar sem a necessidade de realizar algum tipo de cadastro ou instalação como pré-requisito para acesso aos dados.

5.1.2 Contratos Inteligentes

Foi criado um contrato inteligente para gerenciar os dados educacionais na *blockchain*. O Código 1 apresenta a parte principal do código Solidity do contrato inteligente criado. O código completo do contrato está disponível em um repositório[1].

```
1 pragma solidity ^0.4.26;
2 contract ControlEntity{
3 struct Government {
4     string name;
```

[1] <https://github.com/siwelligton/Application-Educ-Dapp>

```
5       uint256 id;
6       string password;
7   }
8   struct EducationInstitution {
9       string nameInstitution;
10      uint256 cnpj;
11      string password;
12      bool statusRecognized;
13  }
14  struct StudentDiploma {
15      string nameInstitution;
16      uint256 cnpjInstitution;
17      string nameStudent;
18      uint256 cpf;
19      string codeMecCurso;
20      string dateAdmission;
21      string dateConclusion;
22  }
23  mapping(uint256 => StudentDiploma) students;
24  uint256[] public studentIds;
25  function registerStudentDiploma(string memory nameInstitution, uint256
        cnpjInstitution,string memory nameStudent,uint256 cpf, string memory
        codeMecCurso,string memory dateAdmission,string memory dateConclusion) public {
26      StudentDiploma storage newStudent = students[cpf];
27      newStudent.nameInstitution = nameInstitution;
28      newStudent.cnpjInstitution = cnpjInstitution;
29      newStudent.nameStudent = nameStudent;
30      newStudent.cpf = cpf;
31      newStudent.codeMecCurso = codeMecCurso;
32      newStudent.dateAdmission = dateAdmission;
33      newStudent.dateConclusion = dateConclusion;
34      studentIds.push(cpf);
35      }
36  function getStudentDiploma(uint256 cpf) public view returns (string memory,uint256,
        string memory,uint256,string memory,string memory, string memory){
37          StudentDiploma storage s = students[cpf];
38          return (s.nameInstitution,s.cnpjInstitution,s.nameStudent,s.cpf,s.
                codeMecCurso,s.dateAdmission,s.dateConclusion);
39      }
40  }
```

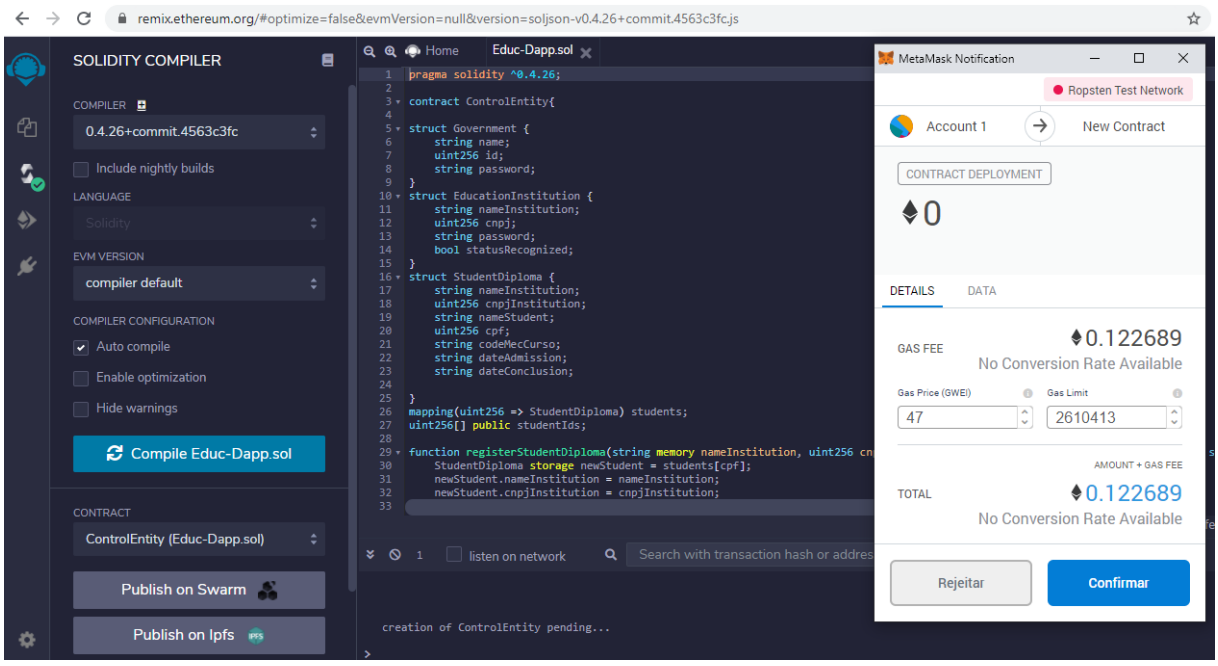
Código-fonte 1 – Código Solidity do contrato inteligente.

O contrato inteligente apresentado possui três estruturas de controle, uma para armazenar a entidade governo, outra para armazenar as instituições educacionais e uma para armazenar os dados dos diplomas dos alunos. Existe o método que registra os diplomas na

blockchain, em que recebe os dados definidos que devem ser armazenados e existe o método que recupera os dados dos diplomas para validação da consulta. Após criação e implantação do contrato inteligente na Ethereum, o *front-end* da aplicação realiza a comunicação com a camada *blockchain* para exibição do resultado das consultas realizadas.

Para implantação do contrato inteligente foi utilizado o *plugin* MetaMask, que funciona como um intermediário para realizar transações na rede *blockchain*. No caso desse protótipo, foi utilizada a rede pública Ropsten, classificada como *testnets*, que utilizam *ethers* fictícios para realizar operações, podendo experimentar diferentes funcionalidades antes de publicar contratos na rede principal (*mainnet*). Através de uma conta criada nesse *plugin* o usuário autoriza ou não as transações na *blockchain*, podendo gerenciar todas transações através dessa conta. A Figura 19 apresenta o momento da implantação do contrato, onde o MetaMask solicita confirmação para executar a operação.

Figura 19 – Operação de implantação do contrato inteligente na IDE Remix com integração com plugin MetaMask



Fonte: o autor.

No momento da implantação do contrato o valor médio de *Gwei* (unidade de medida na qual o *gas* é contabilizado) informado para realizar transações foi 47. Apesar de utilizar uma rede de testes da plataforma Ethereum para realizar a transação, o valor de *Gwei* foi coletado de um site[2] que monitora o ambiente real da Ethereum. Assim o valor em *ether* gasto na transação será gerado de acordo com a situação atual do mercado de *criptomoeda* da Ethereum. Os valores

[2] <https://etherscan.io/gastracker>

de *gas* e *ether* foram 2610437 e 0,122691 respectivamente. O tempo de mineração do bloco foi de 10 segundos. Com a implantação do contrato na *blockchain* Ethereum é possível configurar o endereço do contrato criado no *front-end* para realizar as interações definidas no contrato através da interface Web.

5.1.3 Aplicação Web

Após implantação do contrato inteligente foi desenvolvido o *front-end* da aplicação (Educ-Dapp) que tem integração com a camada *blockchain* para acesso ao contrato. Para programação do *front-end* foi utilizada a IDE Visual Studio Code e a documentação da web3 JavaScript Dapp API. A documentação sobre essa API está disponível nesse link[3]. Foi criado um domínio[4] temporário somente para validar a aplicação. A Figura 20 apresenta a página inicial com algumas informações sobre a aplicação.

Figura 20 – Página principal da aplicação Educ-Dapp

Fonte: o autor.

A Figura 21 apresenta a página de *login* da aplicação, onde somente as entidades

[3] <https://web3js.readthedocs.io/>
[4] <http://ufcpcompquixada.epizy.com/index.html>

Governo e IES poderão entrar na aplicação para executar as transações.

Figura 21 – Página de *login* da aplicação Educ-Dapp

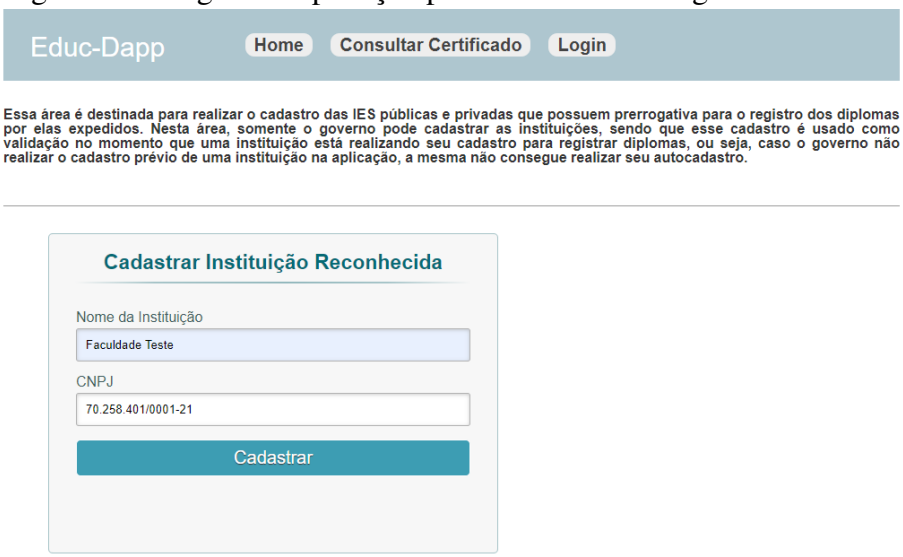
Fonte: o autor.

A Figura 22 apresenta a página da área do Governo. Essa página é para cadastrar as instituições para serem reconhecidas, ou seja, terem a permissão para cadastrar e revogar diplomas na aplicação. Por se tratar de um protótipo, o cadastro foi simplificado para informar somente o nome e CNPJ da instituição. A principal intenção de envolver diretamente a entidade Governo na aplicação é uma forma de propor um processo global que envolva as principais entidades ligadas ao processo de emissão e registros de certificados das IES. Essa é uma forma de controle para simular a interação de órgãos públicos (MEC) com aplicação.

Qualquer IES pode realizar um autocadastro na aplicação para ter direito a registrar os diplomas, mas é necessário antes um cadastro prévio informado pelo Governo, pois a aplicação faz uma validação verificando se a mesma tem o cadastro prévio. Dessa maneira, impede que uma IES irregular realize seu autocadastro e consequentemente o cadastro de diplomas na aplicação. A Figura 23 apresenta a página que as IES realizam o autocadastro na aplicação.

As Figuras 24 e 25 apresentam as páginas de cadastrar e revogar diplomas. Na página de cadastro alguns campos relacionados ao diploma são apresentados para preenchimento. As pessoas podem preencher os campos com as informações de um ou mais diplomas e em seguida clicar em “Adicionar ao Lote” para adicionar os dados ao lote que serão enviados para *blockchain*. Pode-se adicionar ao lote quantos diplomas forem necessários. Após informar todos os dados dos diplomas, será necessário clicar em “Cadastrar”. Dessa forma, a aplicação

Figura 22 – Página da aplicação para cadastrar IES regular



Fonte: o autor.

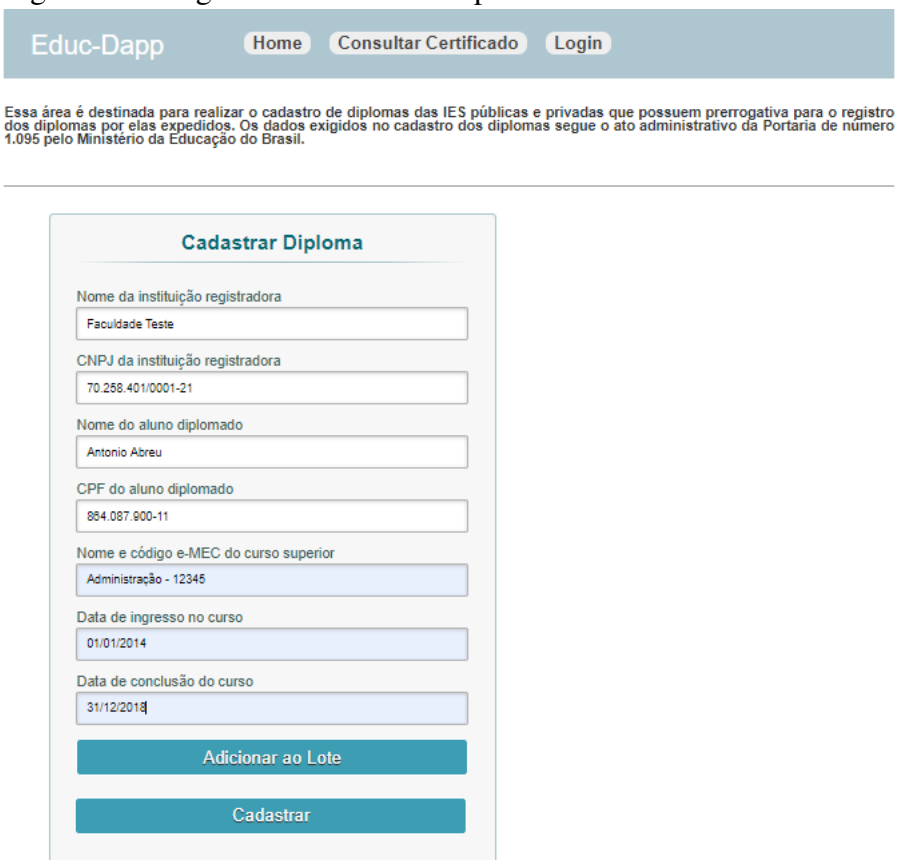
Figura 23 – Página de autocadastro da IES

Fonte: o autor.

vai executar uma única operação de cadastrar, em que será enviado um lote de diplomas para *blockchain*, simulando uma colação de grau que geralmente ocorre no fim do semestre letivo em uma IES e que envolve a emissão e registros de diplomas de vários alunos. Em relação a função revogar um diploma, ela significa corrigir o mesmo, por motivos de erros ou fraude nos dados informados no cadastro realizado na aplicação.

A Figura 26 apresenta a página do resultado de uma busca por um diploma, no qual é realizada a consulta usando o CPF do aluno. Nessa página, aplicação busca na *blockchain* a existência de um diploma com um determinado CPF, que caso positivo o sistema apresenta uma mensagem confirmando a validação com sucesso e exibindo os dados do diploma que foram

Figura 24 – Página de cadastro de diploma



Fonte: o autor.

Figura 25 – Página de revogação de diploma

Fonte: o autor.

registrados.

O código completo da aplicação desenvolvida se encontra em um repositório[5]. Um manual de utilização da aplicação é fornecido no Apêndice B.

5 <https://github.com/siwelligton/Application-Educ-Dapp>

Figura 26 – Página de consulta e resultado da busca por diploma na *blockchain*

Fonte: o autor.

5.2 Cenário de Avaliação

Para ilustrar o funcionamento da arquitetura, foi definido um cenário de utilização para algumas instituições de ensino superior realizarem a avaliação. Os usuários participantes foram pessoas com experiência nos processos administrativos educacionais que envolvem os diplomas. Os dados utilizados na avaliação foram fictícios, pois se tratava de uma simulação. Porém, apesar dos dados serem fictícios, os mesmos foram estruturados e formatados de acordo com o ato administrativo da Portaria nº 1.095 do MEC.

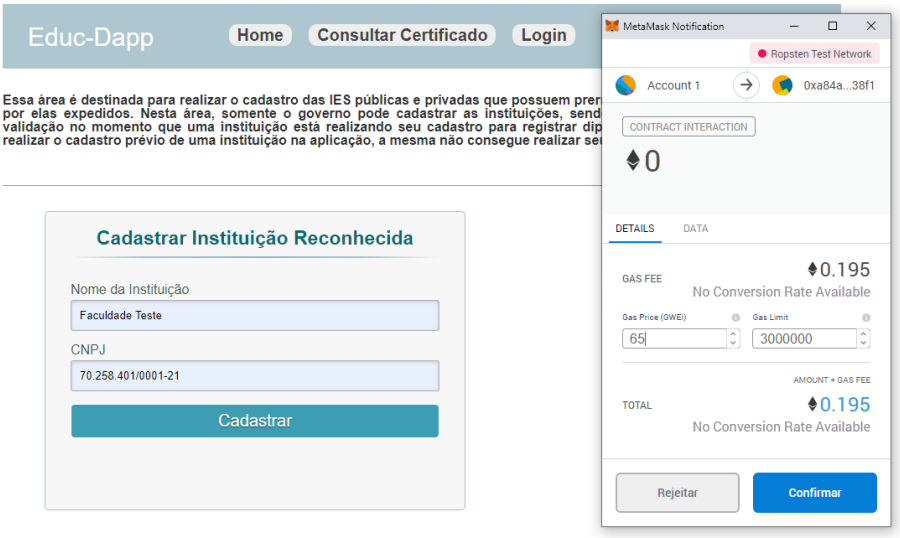
A participação dos usuários ocorreu de forma voluntária e as informações explicando o objetivo da pesquisa foram enviadas por e-mail aos participantes. Também foram enviadas todas as informações necessárias para participar da pesquisa, em que destacam-se os seguintes pontos para participação:

- Ler o ato administrativo da Portaria nº 1.095 do MEC para entender melhor a pesquisa;
- Instalar e configurar a extensão MetaMask no navegador (um manual de instalação do MetaMask é fornecido no Apêndice A);
- Validar a aplicação criada; e
- Responder um questionário para obter informações relacionadas a pesquisa.

Todas as interações da avaliação foram realizadas na aplicação Educ-Dapp que representa a interface do usuário. Para utilizar aplicação desenvolvida foi necessário instalar o

plugin MetaMask no navegador, pois nele foi criado uma carteira de *criptomoeda* para interagir com aplicação. Qualquer transação que insere dados na *blockchain* passa pela aprovação do MetaMask. No início da avaliação cada participante realizou o cadastro de uma instituição fictícia utilizando o perfil do governo. Dessa forma, ela possui autorização para realizar o autocadastro e tem permissão para registrar diplomas na aplicação. A Figura 27 apresenta a tela dessa funcionalidade sendo executada com a confirmação do MetaMask.

Figura 27 – Cadastro de IES regular com confirmação do MetaMask



Fonte: o autor.

Em seguida os participantes realizam o cadastro da instituição com os dados básicos nome e CNPJ. Pode-se observar na Figura 28 o momento da execução dessa transação, em que o MetaMask pede a confirmação para executar essa operação. Após finalizado o cadastro com sucesso, os participantes realizaram *login* para iniciar o processo de cadastro de diplomas na aplicação.

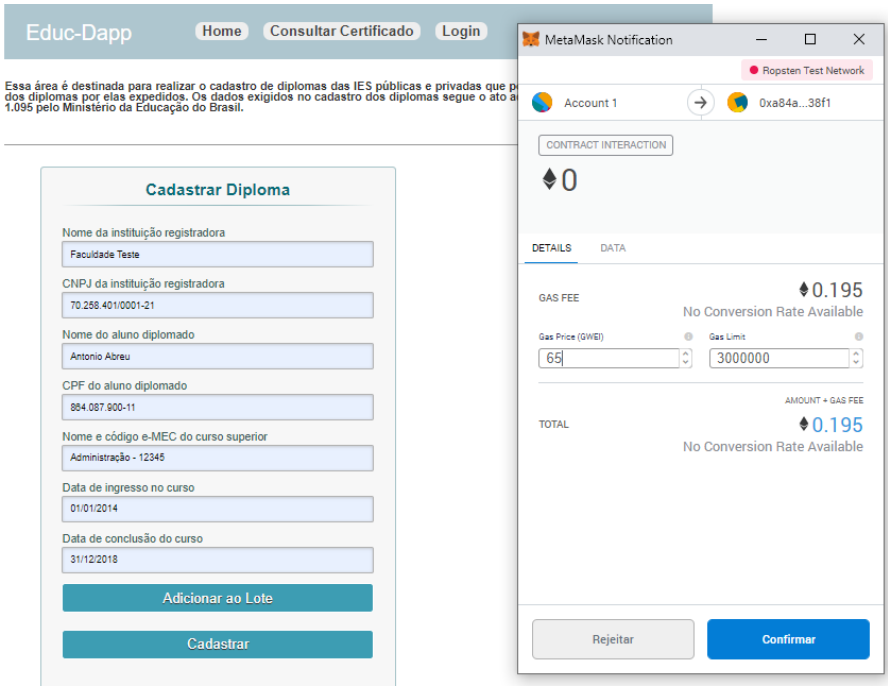
Na tela de cadastros de diplomas cada participante pode informar a quantidade de diplomas que achar necessário para entender o dinamismo da aplicação. A Figura 29 apresenta um exemplo do momento da execução dessa funcionalidade. Também tem a solicitação de confirmação do MetaMask, pois se trata de uma inserção de dados na *blockchain*.

Após execução do cadastro dos diplomas, os dados ficarão disponíveis para serem consultados na *blockchain*. A Figura 26 apresenta um exemplo do momento da consulta usando um CPF fictício de um aluno. Para utilizar essa funcionalidade não é necessária nenhuma confirmação por parte do MetaMask, pois se trata apenas de uma consulta na *blockchain*. Dessa forma, essa funcionalidade é pública e qualquer entidade pode acessá-la sem a necessidade de

Figura 28 – Autocadastro da IES com confirmação do MetaMask

Fonte: o autor.

Figura 29 – Cadastro de diploma realizado pela IES



Fonte: o autor.

instalação do MetaMask.

5.2.1 Projeto

O objetivo desta avaliação com usuários da aplicação é ter um *feedback* sobre o uso da aplicação Educ-Dapp e sua adequação às atividades relacionadas ao armazenamento dos dados e consulta de diplomas. Para atender este objetivo, um questionário *online* foi projetado para a obtenção de dados, apresentado na Tabela 3, composto por três grupos de questões: questões

demográficas, para se identificar o perfil de quem responde à pesquisa; questões sobre a aplicação, sobre a utilização da aplicação e avaliação da solução; e questões de opinião, com questões abertas de texto livre para expressar opinião, sugestões e melhorias. No início do questionário foi apresentado um Termo de Consentimento Livre e Esclarecido (TCLE) explicando o objetivo da pesquisa e pedia que o participante concordasse antes de prosseguir para as perguntas.

Tabela 3 – Questões demográficas (QD), sobre a aplicação (QA) e de opinião (QO) do questionário

ID	Descrição
QD1	Qual é o seu nome?
QD2	Qual é o seu e-mail?
QD3	Qual é a sua afiliação?
QD4	Qual seu nível de escolaridade?
QD5	Qual é a sua área de atuação?
QD6	Qual é a sua experiência profissional?
QD7	Qual é a sua experiência com certificados?
QD8	Sua instituição utiliza alguma solução tecnológica que fornece mecanismos para disponibilizar uma consulta de certificados?
QD9	Você conhece a portaria 1.095 expedida pelo Ministério da Educação?
QD10	Você conhece blockchain?
QA1	De 1 a 5, qual o nível de facilidade de uso da aplicação criada?
QA2	De 1 a 5, qual o nível de navegação da aplicação criada?
QA3	De 1 a 5, qual a percepção do tempo de consulta de um diploma?
QA4	De 1 a 5, qual a percepção do tempo para executar o cadastro de diplomas?
QA5	A aplicação criada atende aos requisitos da portaria 1.095 expedida pelo Ministério da Educação?
QA6	Existem diferenças significativas entre aplicação criada e uma aplicação tradicional?
QO1	Quais os pontos fortes da aplicação?
QO2	Quais os pontos fracos da aplicação?
QO3	Quais suas sugestões de melhorias para a aplicação?

Fonte: o autor.

Nas questões demográficas solicitou-se o nome, e-mail e afiliação do respondente. Por afiliação entende-se a IES que trabalha. Quanto ao nível de escolaridade, as opções foram: Ensino Médio, Estudante de Graduação, Graduação, Especialização, Estudante de Mestrado, Mestrado, Estudante de Doutorado e Doutorado. A área de atuação corresponde ao cargo exercido na IES que trabalha. A experiência profissional é o tempo de trabalho em IES, variando de nenhuma, menos de 1 ano, de 1 a 5 anos, de 5 a 10 anos, de 10 a 15 anos e mais que 15 anos. A experiência com certificados se refere ao conhecimento sobre o processo de emissão e registro de certificados das IES, variando também de nenhuma, menos de 1 ano, de 1 a 5 anos, de 5 a 10 anos, de 10 a 15 anos e mais que 15 anos. Em relação à solução tecnológica, é qualquer tipo de sistema, ferramenta ou aplicação web desenvolvido pela própria instituição ou de terceiros para disponibilizar uma consulta pública para qualquer entidade verificar os certificados emitidos, sendo apenas opções sim e não. Sobre conhecer a portaria 1.095 expedida

pelo MEC, é especificamente se conhecia antes da realização deste estudo, sendo também sim e não. Por fim, em relação a conhecer *blockchain*, é ter visto algo a respeito dessa tecnologia em notícias ou estudos pessoais, ou seja, não necessariamente tenha que ter conhecimento técnico dessa tecnologia, com opções variando entre "Eu não conheço essa tecnologia", "Eu tenho pouco conhecimento dessa tecnologia", "Eu tenho conhecimento intermediário nessa tecnologia" e "Eu tenho conhecimento avançado nessa tecnologia".

Nas questões sobre a aplicação, analisou-se o uso da aplicação. Por facilidade de uso definiu-se como a capacidade da aplicação em fornecer ao usuário um fluxo de fácil compreensão para executar as funções da aplicação, variando de difícil a fácil, sendo 1 a menor pontuação e 5 a máxima. O nível de navegação foi a facilidade ou dificuldade de navegar entre as páginas *web* da aplicação, também variando de difícil a fácil. A percepção do tempo de consulta de um diploma se referiu ao tempo de resposta da aplicação para apresentar os dados na tela da consulta realizada, variando de muito lenta a rápida, sendo 1 a menor pontuação e 5 a máxima. Por percepção do tempo para executar o cadastro de diplomas definiu-se o tempo de resposta da aplicação para finalizar o cadastro de um ou vários diplomas. Não é para levar em consideração o tempo para preencher o formulário com os dados do certificado, ou seja, é para considerar o tempo a partir do clique no botão para cadastrar, variando também de muito lenta a rápida. A aplicação criada atende aos requisitos da portaria 1.095 expedida pelo MEC teve opções "Não", "Talvez", "Parcialmente" e "Totalmente". E se existem diferenças significativas entre aplicação criada e uma aplicação tradicional também teve opções "Não", "Talvez", "Parcialmente" e "Totalmente". Sendo que essas diferenças significativas estão relacionadas a percepção de uso das funções e navegação na aplicação criada.

As questões demográficas e sobre a aplicação serão analisadas de maneira quantitativamente por meio de gráficos, comparação de valores absolutos e porcentuais. Já as questões de opinião serão analisadas de maneira qualitativamente.

5.2.2 Avaliação com Usuários

A avaliação contou com dez participantes. O período da execução foi entre os dias 22/09/2020 e 07/10/2020. Todos possuem experiência no processo de emissão de certificados. Inclusive alguns customizaram sistemas para tratar desse processo ou implantaram o processo que gerencia a emissão de certificados em uma IES. Para analisar o perfil, percepção e opinião dos participantes sobre a solução proposta segue a seguir as respostas do questionário aplicado.

QD3 - Qual é a sua afiliação? A avaliação teve 10 participantes de 5 IES distintas. Destas IES, 4 instituições são privadas e apenas 1 pública. As IES estão localizadas em 3 cidades diferentes do Estado do Ceará.

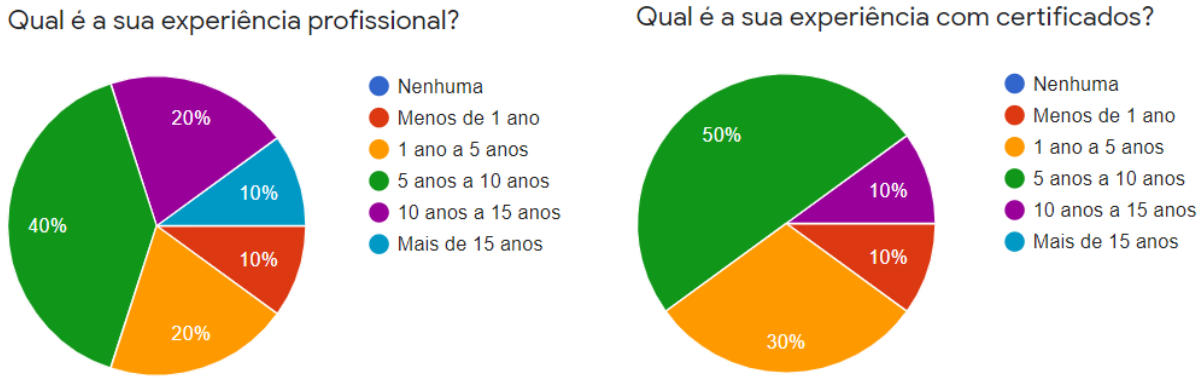
QD4 - Qual seu nível de escolaridade? Foram 7 participantes com especialização, 2 com graduação e 1 estudante de mestrado.

QD5 - Qual é a sua área de atuação? A área de atuação dos participantes em relação ao cargo que exerce na IES que trabalha estão distribuídas da seguintes forma: (i) dois são analistas de TI; (ii) um analista de sistemas; (iii) um analista de processos; (iv) um analista educacional; (v) um supervisor de TI; (vi) um professor; (vii) um administrador; (viii) um assistente em administração; e (ix) um auxiliar administrativo.

QD6 - Qual é a sua experiência profissional? A resposta pode ser visualizada na Figura 30 à esquerda. Percebe-se que a maioria dos respondentes possui entre 5 e 10 anos de experiência. 70% dos respondentes possui mais de 5 anos de experiência, o que é bom para a pesquisa pois pode indicar maturidade profissional.

QD7 - Qual é a sua experiência com certificados? A resposta pode ser visualizada na Figura 30 à direita. Percebe-se também que a maioria dos respondentes possui entre 5 e 10 anos de experiência. 60% dos respondentes possui mais de 5 anos de experiência com certificados, o que é bom para a pesquisa pois pode indicar maturidade nos processos de emissão de certificados.

Figura 30 – Questões demográficas sobre experiência profissional e em certificados



Fonte: Elaborada pelo autor.

QD8 - Sua instituição utiliza alguma solução tecnológica que fornece mecanismos para disponibilizar uma consulta de certificados? 4 responderam não e 6 sim.

QD9 - Você conhece a portaria 1.095 expedida pelo Ministério da Educação? 2 responderam não e 8 sim.

QD10 - Você conhece *blockchain*? 3 responderam não, 3 responderam que possuem conheci-

mento intermediário e 4 possuem pouco conhecimento.

A seguir, o consolidado das questões sobre a aplicação:

QA1 - De 1 a 5, qual o nível de facilidade de uso da aplicação criada? 1 participante marcou o valor 2, 1 marcou o valor 4 e 8 marcaram o valor 5. Assim, a maioria respondeu que a aplicação possui um fluxo de fácil compreensão para executar as funções.

QA2 - De 1 a 5, qual o nível de navegação da aplicação criada? 1 participante marcou o valor 3, 3 marcaram o valor 4 e 6 marcaram o valor 5. Assim, a maioria pontuou uma facilidade na navegação entre as páginas *web* da aplicação.

QA3 - De 1 a 5, qual a percepção do tempo de consulta de um diploma? Todos participantes marcaram o valor 5. Portanto, todos responderam que a aplicação possui tempo de resposta rápido para apresentar os dados na tela da consulta executada.

QA4 - De 1 a 5, qual a percepção do tempo para executar o cadastro de diplomas? 6 participantes marcaram o valor 4 e 4 marcaram o valor 5. Portanto, a maioria dos respondentes apontou que a aplicação possui um tempo de resposta rápido para finalizar o cadastro de um ou vários diplomas.

QA5 - A aplicação criada atende aos requisitos da portaria 1.095 expedida pelo Ministério da Educação? 9 responderam totalmente e 1 parcialmente. Isto implica em que a portaria pode ser plenamente atendida pela aplicação, bastando alguns refinamentos.

QA6 - Existem diferenças significativas entre aplicação criada e uma aplicação tradicional? 7 responderam não e 3 parcialmente. Isto pode implicar que a aplicação necessita de melhorias na interface gráfica do usuário.

A análise das questões de opinião foi conduzida de maneira livre, pois houve poucas respostas. Basicamente foram identificados ao longo dos comentários dos respondentes os destaques. Para uma melhor compreensão e anonimização dos respondentes, cada citação é identificada por um "P" seguido por um número, que indicou a ordem de resposta do questionário.

Os pontos fortes foram descritos na QO1. Destaques para segurança dos dados, disponibilidade do ambiente, acesso aos dados e infraestrutura. A maioria das respostas citou segurança como um benefício. Isso é uma das características da *blockchain*, para preservação dos dados. Um exemplo de menção foi a resposta de P3 em "*Segurança dos dados, replicados em várias máquinas conectadas na rede Ethereum*". Disponibilidade devido à natureza da *blockchain* também foi citada, como no comentário de P2 com "*Possibilidade de Manter os dados distribuídos garantindo a disponibilidade e segurança dos dados ...*". O acesso aos dados,

seja por facilidade, seja por rapidez, também foi destacado, como citado por P7 em "*Rapidez das ações, facilidade de busca dos diplomas, facilidade de uso em geral*". Por fim, fato da possibilidade de não precisar de uma infraestrutura local, seja por recursos físicos ou financeiros, e tudo concentrado em um só ambiente, foi destacado por P6 em *Não existe a necessidade de manutenção tradicional de bancos de dados relacional ... Existe uma economia financeira em relação a infraestrutura montada para manter o serviço disponível*".

Como pontos fracos, QO2 apresentou menções ao uso do MetaMask, a custos relacionados ao uso da aplicação e sobre a ausência de algumas funcionalidades. Em relação ao MetaMask, ele é necessário para autorizar as transações e ter um controle das operações executadas na rede Ethereum. Também houve menção a não haver pontos fracos. Mesmo assim, muitas respostas foram em relação ao seu uso, como um ponto fraco da aplicação, como no comentário de P5 com "*Depender de um serviço terceiro (MetaMask)*". Custos para quem trabalha com *blockchain* é um aspecto de importância. Alguns comentários foram no sentido de alertar sobre isso, como P3 em "*O custo pode ser bastante alto da aplicação (avaliar o custo); É necessário conhecer um pouco de blockchain e seu funcionamento, através de criptomoedas; Deve melhorar para não restarem dúvidas para as pessoas das IES que irão manipular o sistema*". Por fim, algumas funcionalidades, como melhorias nos cadastros e importação de dados foram ressaltadas, como na resposta de P8 com "*não importar em lote via arquivo txt ou csv, não ter integração com outros sistemas do mercado*".

Por fim, QO3 destacou as sugestões de melhoria para a aplicação. Os destaques foram para o uso do MetaMask na aplicação, para usabilidade e interface do usuário de maneira geral, e sugestão de novas funcionalidades. A utilização do MetaMask é um mecanismo para acesso a rede Ethereum, sendo necessário seu uso em ambientes de testes e produção, assim como apontado nos pontos fracos, também foi apontado por vários respondentes. Nesse caso, como sugestão de melhoria para o usuário final não ter que utilizá-lo, ou utilizá-lo de maneira transparente, como no comentário de P1 em "*Justamente o uso do MetaMask ser transparente para o usuário*" e P2 com "*Deixar o plugin MetaMask transparente nas operações do sistema; Funcionalidade de importação de arquivo (.csb, .txt ou .json) para o cadastro de diplomas*". P2 também destacou sobre a funcionalidade de importação de arquivos em formatos variados com os dados dos diplomas como uma melhoria. Questões de usabilidade, navegação, aspectos da interface gráfica do usuário também foram comentados, como na resposta de P3 com "*Usabilidade deve melhorar; o fluxo de processos; implementar outras funções básicas;*". Por

fim, funcionalidades gerais foram sugeridas, como relatório no discurso de P5 com "*Implementar relatórios de consulta...*" e na resposta de P9 com "*No ambiente da Instituição, ao cadastrar o diploma, já incluir os campos nome e CNPJ da faculdade. Poderia também já vir cadastrado a lista dos cursos*".

5.3 Avaliação de Desempenho

O objetivo dessa avaliação do desempenho é analisar a aplicação do ponto de vista de infraestrutura, especificamente da *blockchain* e custos.

5.3.1 Projeto do Experimento

O projeto do experimento baseou-se nas atividades descritas em Jain (1991). O planejamento da análise de desempenho teve a mesma infraestrutura e ambiente utilizados na avaliação da aplicação com usuários descritos na seção 5.1.1.

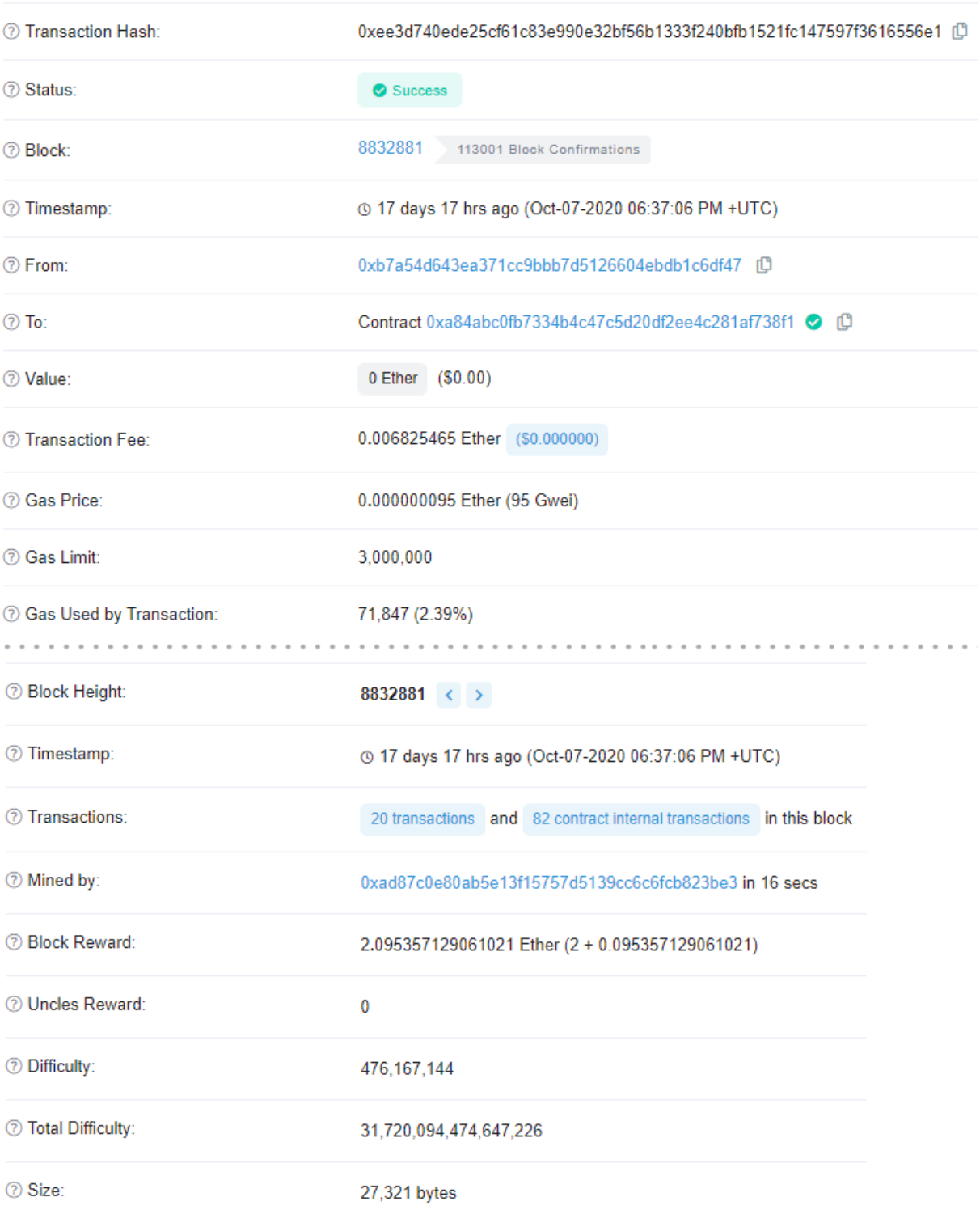
A técnica de análise de desempenho utilizada é a medição, com coleta de dados baseada nas informações fictícias inseridas pelos participantes na aplicação. A coleta dos dados ocorreu durante a utilização da aplicação pelos avaliadores, que conforme as ações eram executadas, os dados eram obtidos através da ferramenta Etherscan, onde são armazenados e posteriormente coletados e consolidados. Por meio dessa ferramenta é possível analisar todas as transações realizadas, tendo informações detalhadas sobre os blocos criados. A Figura 31 apresenta os detalhes de um bloco criado em uma transação da avaliação.

Durante a avaliação os participantes utilizaram o valor médio de *Gwei* nas transações informado no site[6] que monitora o ambiente real da Ethereum. Dessa forma, mesmo utilizando uma rede de testes da Ethereum para executar as transações, os valores de *ether* gastos nas transações serão gerados de acordo com a situação atual do mercado de *criptomoeda* da Ethereum. O *Gwei* é a unidade de medida na qual o *gas* é contabilizado, consequentemente utilizado para calcular o valor em *ether* para executar determinada transação. Foi observado que durante o uso da aplicação os valores de *Gwei* informados considerando da primeira a última avaliação foram respectivamente 65, 58, 63, 110, 59, 105, 78, 67, 97 e 95.

Os dados coletados e consolidados são apresentados sob a forma de histogramas e *boxplots* e os seguintes valores estatísticos serão calculados: valor máximo, valor mínimo, média, mediana, variância, desvio padrão e primeiro e terceiro quartis.

6 <https://etherscan.io/gastracker>

Figura 31 – Detalhes de um bloco criado na blockchain



Fonte: o autor.

Um histograma é um gráfico de frequência que tem por objetivo ilustrar como uma determinada amostra ou população de dados está distribuída. Ele é constituído por retângulos ou linhas, desenhados a partir de uma linha na base, na qual suas posições ao longo dessa linha representam o valor, amplitude ou altura da variável. Um *boxplot* ou diagrama de caixa, é um

gráfico no qual o eixo vertical representa a variável a ser analisada e o eixo horizontal representa um fator de interesse. É uma ferramenta para localizar e analisar como uma variável está variando entre diferentes grupos de dados. É utilizado também para se identificar onde estão localizados 50% dos valores mais prováveis, a mediana e os valores extremos.

A mediana é o valor que separa a metade maior e a metade menor de uma amostra, uma população ou uma distribuição de probabilidade. O desvio padrão é uma medida de dispersão, ou seja, qual a distância dos dados de uma amostra com relação à média. Um baixo desvio padrão indica que os pontos dos dados tendem a estar próximos da média ou do valor esperado. Um alto desvio padrão indica que os pontos dos dados estão espalhados por uma ampla gama de valores. Em relação aos quartis, destacamos o primeiro quartil que representa o valor do conjunto que delimita os 25% dos valores menores e o terceiro quartil representa o valor do conjunto que delimita os 75% dos valores menores de uma amostra.

A Tabela 4 exibe um resumo do projeto do experimento. As métricas coletadas do experimento são: *ether*, *gas* e tempo de mineração do bloco.

Tabela 4 – Critérios para avaliação de desempenho para os experimentos

Critério	Descrição
Sistema	Um ambiente composto por uma aplicação web que acessa dados de uma *blockchain*
Métricas	*ether*, *gas*, tempo para minerar os blocos
Parâmetros	Não haverá variação de configurações do ambiente
Fatores	Não haverá repetições dos experimentos, pois depende da quantidade de acessos dos usuários
Técnica de Avaliação	Medição
Carga de Trabalho	Cargas geradas pela utilização do sistema pelos usuários
Projeto de Experimentos	Geração de cargas de trabalho pelos usuários conforme roteiro pré estabelecido, coleta dos dados (métricas) pela ferramenta Etherscan para consolidação dos resultados
Análise dos dados	Geração dos dados estatísticos (valor máximo, valor mínimo, média, mediana, desvio padrão, primeiro e terceiro quartis) e gráficos (histograma e *boxplot*), e análise dos resultados

Fonte: o autor.

5.3.2 Execução

As subseções a seguir apresentam os gráficos e tabelas consolidando os resultados. Elas estão separadas pelas seguintes funcionalidades da aplicação analisadas: cadastro, revogação, correção e consulta.

Todas as figuras de *boxplot* das subseções a seguir possuem alguns losangos coloridos.

O losango vermelho indica a média, o azul a mediana, e o verde o desvio padrão. Esses valores estão disponibilizados também nas tabelas. Adicionalmente, alguns valores estatísticos foram calculados para complementar as análises, que foram valor mínimo, valor máximo, média, mediana, quartis e desvio padrão. Todos os valores de *ether* foram informados somente até a quarta casa decimal após a vírgula para facilitar a visualização dos dados. Os valores de tempo também foram informados apenas até a segunda casa decimal após a vírgula.

Para ter uma visualização financeira na moeda brasileira para cada funcionalidade da aplicação, foi realizado uma conversão no final de cada subseção de valores da *criptomoeda* para dólar e em seguida para o real brasileiro. No momento da escrita deste texto, 1 *ether* estava valendo US$ 407,47, correspondendo a R$ 2289,98, sendo que a cotação estava R$ 5,62 para US$ 1,00. O monitoramento da cotação da *criptomoeda* da Ethereum pode ser acompanhado através do site do Etherscan[7].

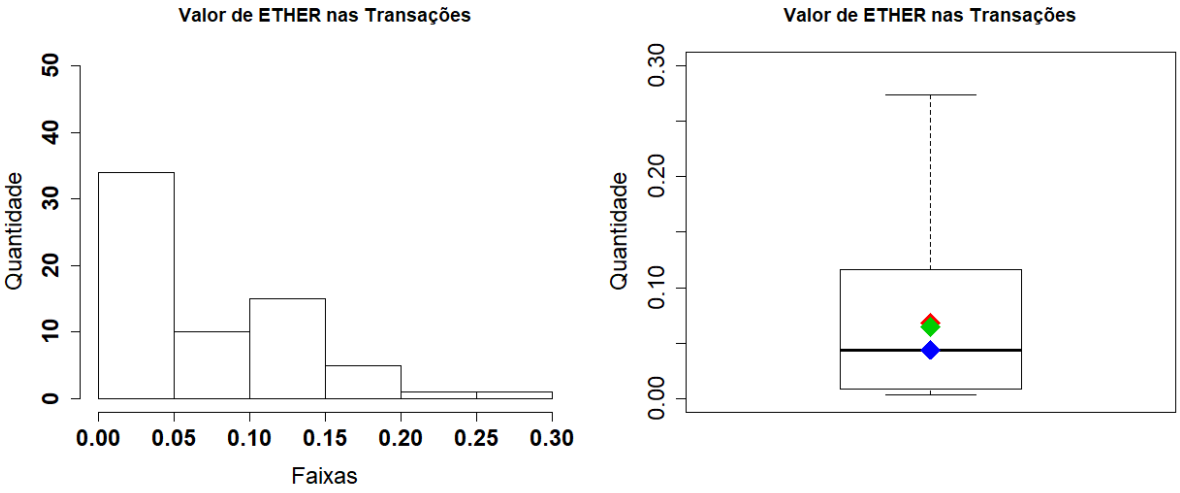
5.3.3 Cadastro de Diplomas e Instituições

A Figura 32 exibe o histograma e *boxplot* para os valores de *ether* coletados da funcionalidade cadastrar diploma. O menor valor coletado foi 0,0032 e o maior foi 0,2738, ou seja, os valores de *ether* gastos nesse tipo de transação estão entre esse intervalo. A mediana foi 0,0439 *ether*, ou seja, metade das transações ocorreram com um valor menor que 0,0439 *ether* e a outra metade ocorreram com valor maior que 0,0439 *ether*. O primeiro quartil do *boxplot* tem o valor de 0,0089 *ether*, ou seja, um quarto das transações foram com um valor menor que 0,0089 *ether*. Já o terceiro quartil do *boxplot* tem valor de 0,1162 *ether*, ou seja, 75% das transações ocorreram com valor menor que 0,1162 *ether*. Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (0,2738 - 0,0032) é de 0,2706 *ether*. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de *ether* gasto nas transações.

A Figura 33 exibe o histograma e *boxplot* para os valores de *gas* coletados da funcionalidade cadastrar diploma. O menor valor coletado foi 17958 e o maior foi 2607892, ou seja, os valores de *gas* gastos nesse tipo de transação estão entre esse intervalo. A mediana foi 616901 *gas*, ou seja, metade das transações ocorreram com um valor menor que 616901 *gas* e a outra metade ocorreram com valor maior que 616901 *gas*. O primeiro quartil do *boxplot* tem o valor de 94519 *gas*, ou seja, um quarto das transações foram com um valor menor que 94519 *gas*.

[7] <https://etherscan.io/>

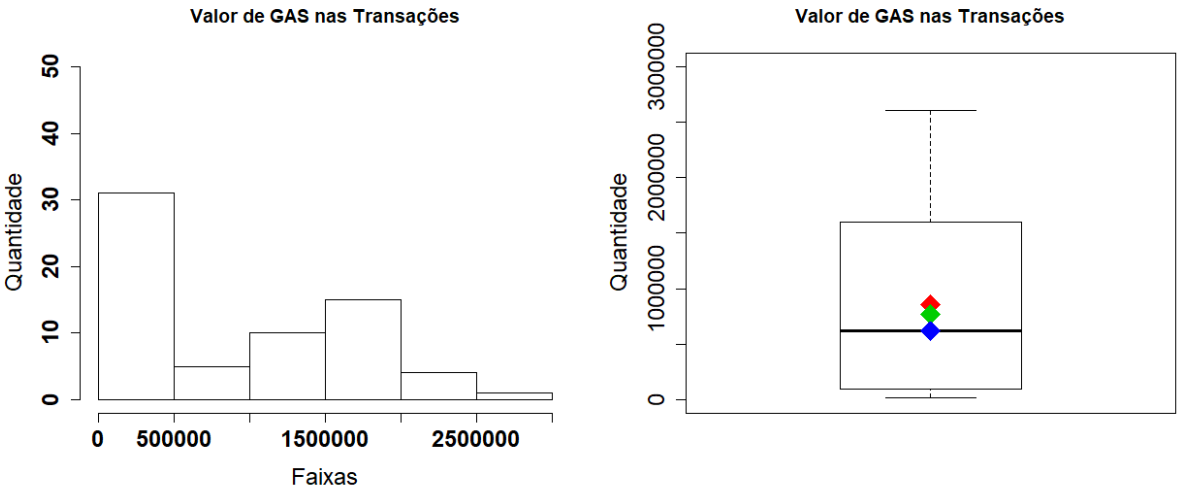
Figura 32 – Histograma e *boxplot* para valores coletados de *ether* da funcionalidade de cadastro de diplomas



Fonte: Elaborada pelo autor.

Já o terceiro quartil do *boxplot* tem valor de 1598291 *gas*, ou seja, 75% das transações ocorreram com valor menor que 1598291 *gas*. Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (2607892 - 17958) é de 2589934 *gas*. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de *gas* gasto nas transações.

Figura 33 – Histograma e *boxplot* para valores coletados de *gas* da funcionalidade de cadastro de diplomas

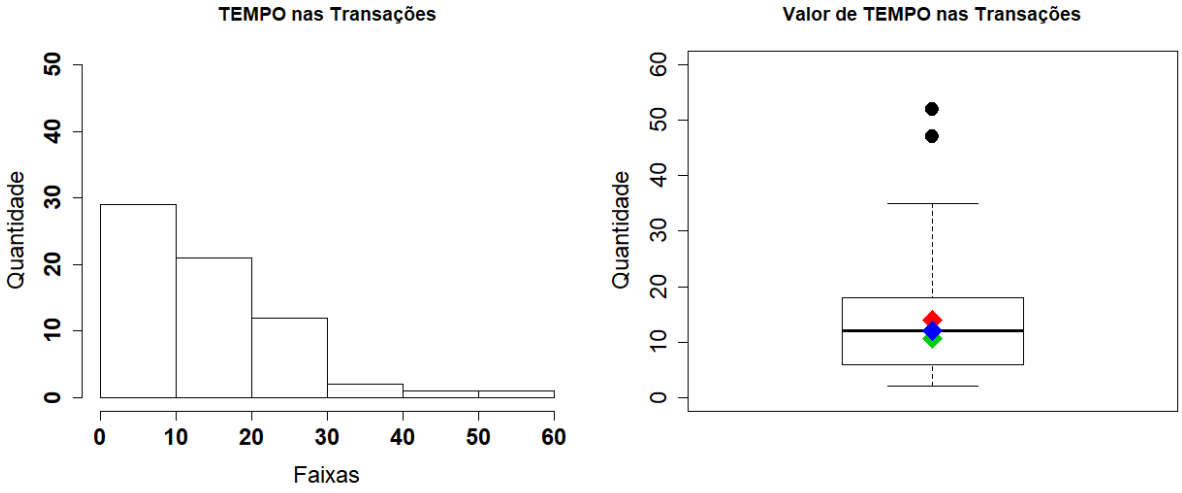


Fonte: Elaborada pelo autor.

A Figura 34 exibe o histograma e *boxplot* para os valores de tempo coletados da funcionalidade cadastrar diploma. Observou-se uma variabilidade de tempo considerável, e a ocorrência de dois *outliers* (transações com tempo de 47 e 52 segundos), que apresentam um

afastamento dos demais valores. Em estatística, *outlier* é considerado um valor aberrante ou valor atípico. É uma observação que apresenta um grande afastamento das demais da série ou é considerada uma inconsistência (DENCKER, 2010). Esses *outliers* identificados foram de transações executadas em momentos que a rede Ethereum estava com instabilidades em seu ambiente. O menor tempo coletado foi 2 segundos e o maior foi 52 segundos, ou seja, os valores de tempo nesse tipo de transação estão entre esse intervalo. A mediana foi 12 segundos, ou seja, metade das transações ocorreram com um tempo menor que 12 segundos e a outra metade ocorreram com tempo maior que 12 segundos. O primeiro quartil do *boxplot* tem o tempo de 6 segundos, ou seja, um quarto das transações foram com um tempo menor que 6 segundos. Já o terceiro quartil do *boxplot* tem tempo de 18 segundos, ou seja, 75% das transações ocorreram com tempo menor que 18 segundos. Neste cenário, pode-se afirmar que o alcance da transação com maior tempo e a de menor tempo (52 - 2) é de 50 segundos. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de segundos gastos nas transações.

Figura 34 – Histograma e *boxplot* para valores coletados do tempo (segundos) para minerar o bloco da funcionalidade de cadastro de diplomas



Fonte: Elaborada pelo autor.

A quantidade de transações executadas pelos participantes da avaliação nessa funcionalidade de cadastrar diplomas foram 66 transações. Muitas dessas transações foram executas com lotes de 1 a 5 diplomas por transação. A Tabela 5 apresenta um resumo dos valores estatísticos coletados da função cadastrar diploma.

De acordo com os resultados obtidos, pode-se observar um crescimento de custos de *ether* e *gas* baseado na quantidade e tamanho dos dados usado na transação, ou seja, quanto mais

Tabela 5 – Valores estatísticos para a funcionalidade de cadastro de diploma

Estatística	ETHER	GAS	TEMPO
Valor Mínimo	0,0032	17958	2,00
Valor Máximo	0,2738	2607892	52,00
Média	0,0679	858029	13,95
Mediana	0,0439	616901	12,00
Primeiro Quartil	0,0089	94519	6,00
Terceiro Quartil	0,1162	1598291	18,00
Desvio Padrão	0,0600	772000,30	10,63

Fonte: o autor.

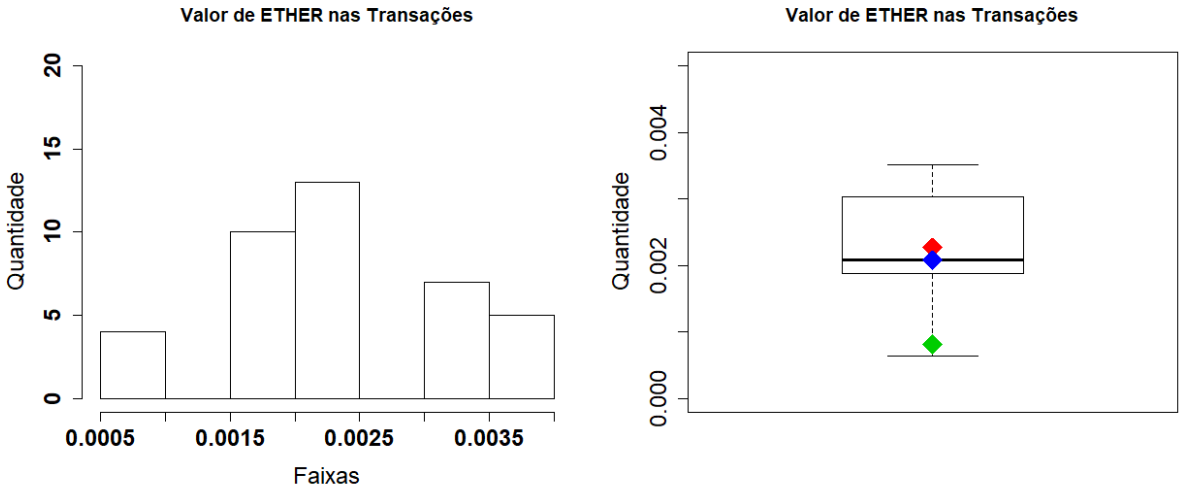
informações forem necessárias para armazenar na *blockchain* maior é o custo computacional e valor em *criptomoeda* para processá-la. Em relação ao tempo, pode-se observar uma variação inconstante do tempo para minerar os blocos das transações. Por exemplo, foram identificadas transações com menos informação para serem armazenadas na *blockchain* que demorou mais tempo para minerar os blocos que uma transação com mais informações para serem processadas. Considerando os valores mínimo, média e máximo de *ether* informados na Tabela 5, os mesmos representam R$ 7,32, R$ 155,48 e R$ 626,99 respectivamente.

5.3.4 Revogação de Diplomas

A Figura 35 exibe o histograma e *boxplot* para os valores de *ether* coletados da funcionalidade revogar diploma. O menor valor coletado foi 0,0006 e o maior foi 0,0035, ou seja, os valores de *ether* gastos nesse tipo de transação estão entre esse intervalo. A mediana foi 0,0020 *ether*, ou seja, metade das transações ocorreram com um valor menor que 0,0020 *ether* e a outra metade ocorreram com valor maior que 0,0020 *ether*. O primeiro quartil do *boxplot* tem o valor de 0,0018 *ether*, ou seja, um quarto das transações foram com um valor menor que 0,0018 *ether*. Já o terceiro quartil do *boxplot* tem valor de 0,0030 *ether*, ou seja, 75% das transações ocorreram com valor menor que 0,0030 *ether*. Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (0,0030 - 0,0006) é de 0,0024 *ether*. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de *ether* gasto nas transações.

A Figura 36 exibe o histograma e *boxplot* para os valores de *gas* coletados da funcionalidade revogar diploma. O valor de *gas* coletado em todas as transações realizadas foi 31947, ou seja, ele foi constante durante todo experimento. Com isso, a mediana, o primeiro e terceiro quartil do *boxplot* ficaram com esse mesmo valor de *gas*. No histograma é possível

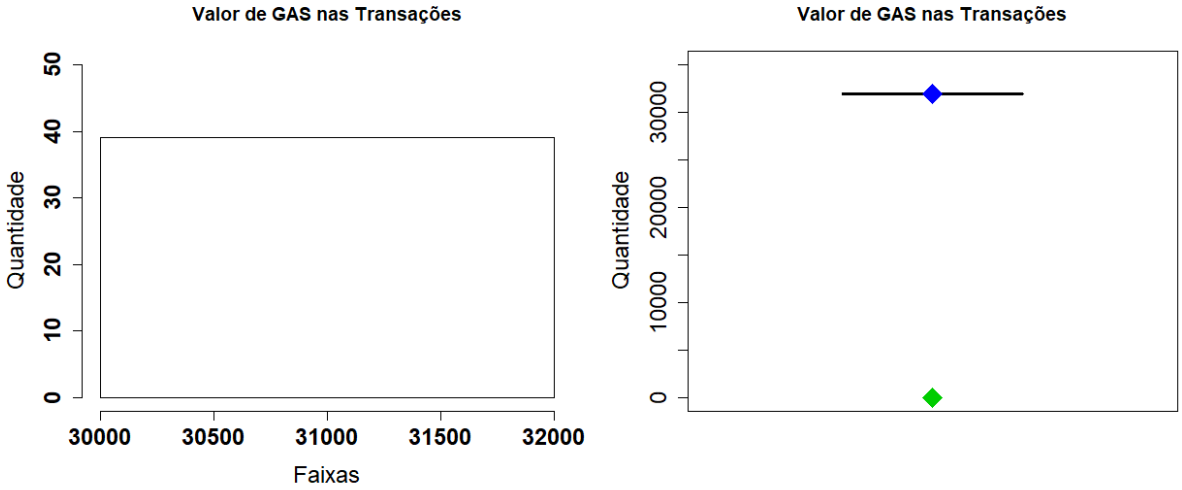
Figura 35 – Histograma e *boxplot* para valores coletados de *ether* da funcionalidade de revogação de diplomas



Fonte: Elaborada pelo autor.

visualizar que todas transações desse tipo foram com o mesmo valor de *gas* gasto nas transações.

Figura 36 – Histograma e *boxplot* para valores coletados de *gas* da funcionalidade de revogação de diplomas

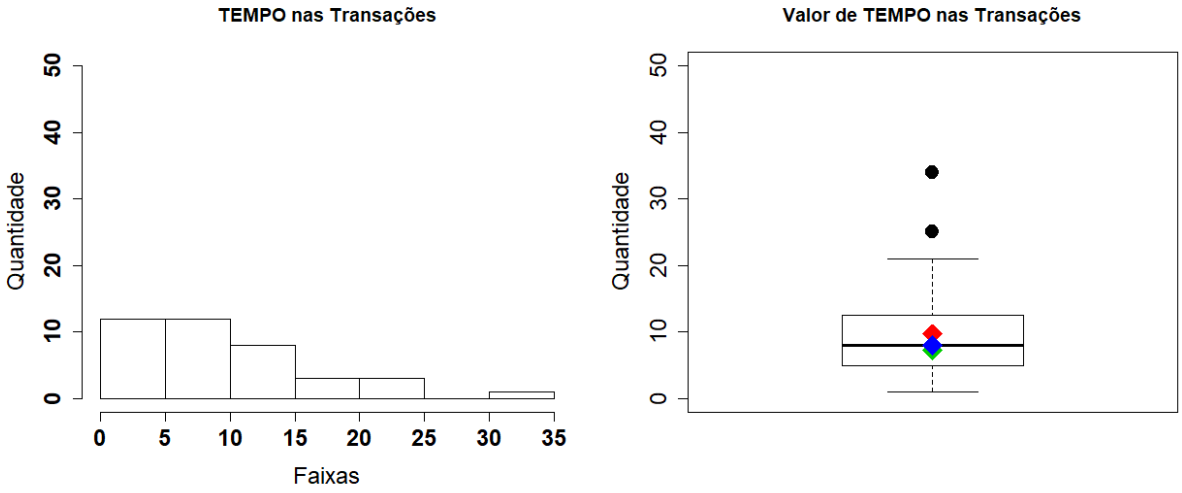


Fonte: Elaborada pelo autor.

A Figura 37 exibe o histograma e *boxplot* para os valores de tempo coletados da funcionalidade revogar diploma. Na execução dessa funcionalidade também percebeu-se uma variabilidade de tempo considerável, e a ocorrência de dois *outliers* (transações com tempo de 25 e 34 segundos), que apresentam um afastamento dos demais valores. Esses *outliers* identificados foram também de transações executadas em momentos que a rede Ethereum estava com instabilidades em seu ambiente. O menor tempo coletado foi 1 segundo e o maior foi 34 segundos, ou seja, os valores de tempo nesse tipo de transação estão entre esse intervalo. A

mediana foi 8 segundos, ou seja, metade das transações ocorreram com um tempo menor que 8 segundos e a outra metade ocorreram com tempo maior que 8 segundos. O primeiro quartil do *boxplot* tem o tempo de 5 segundos, ou seja, um quarto das transações foram com um tempo menor que 5 segundos. Já o terceiro quartil do *boxplot* tem tempo de 12,50 segundos, ou seja, 75% das transações ocorreram com tempo menor que 12,50 segundos. Neste cenário, pode-se afirmar que o alcance da transação com maior tempo e a de menor tempo (34 - 1) é de 33 segundos. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de segundos gastos nas transações.

Figura 37 – Histograma e *boxplot* para valores coletados do tempo (segundos) para minerar o bloco da funcionalidade de revogação de diplomas



Fonte: Elaborada pelo autor.

A quantidade de transações executadas pelos participantes da avaliação nessa funcionalidade de revogar diplomas foram 39 transações. A Tabela 6 apresenta um resumo dos valores estatísticos coletados da função revogar diploma.

Tabela 6 – Valores estatísticos para a funcionalidade de revogação de diploma

Estatística	ETHER	GAS	TEMPO
Valor Mínimo	0,0006	31947	1,00
Valor Máximo	0,0035	31947	34,00
Média	0,0022	31947	9,69
Mediana	0,0020	31947	8,00
Primeiro Quartil	0,0018	31947	5,00
Terceiro Quartil	0,0030	31947	12,50
Desvio Padrão	0,0008	0,00	7,29

Fonte: o autor.

De acordo com os resultados obtidos, pode-se observar um valor constante para o valor de *gas*. Isso se deve pelo formato e tamanho padrão dos dados sempre utilizado no momento de executar essa funcionalidade, ou seja, para executar essa função sempre é utilizado o CPF do aluno, que tem um tamanho e formato único. Em relação ao valor de *ether*, o mesmo tem uma variação devido aos diferentes valores de *Gwei* informados no momento de executar as transações. Em relação ao tempo, pode-se observar uma variação inconstante do tempo para minerar os blocos das transações, mesmo utilizando dados com mesmo tamanho e formato (CPF do aluno). Considerando os valores mínimo, média e máximo de *ether* informados na Tabela 6, os mesmos representam R$ 1,37, R$ 5,03 e R$ 8,01 respectivamente.

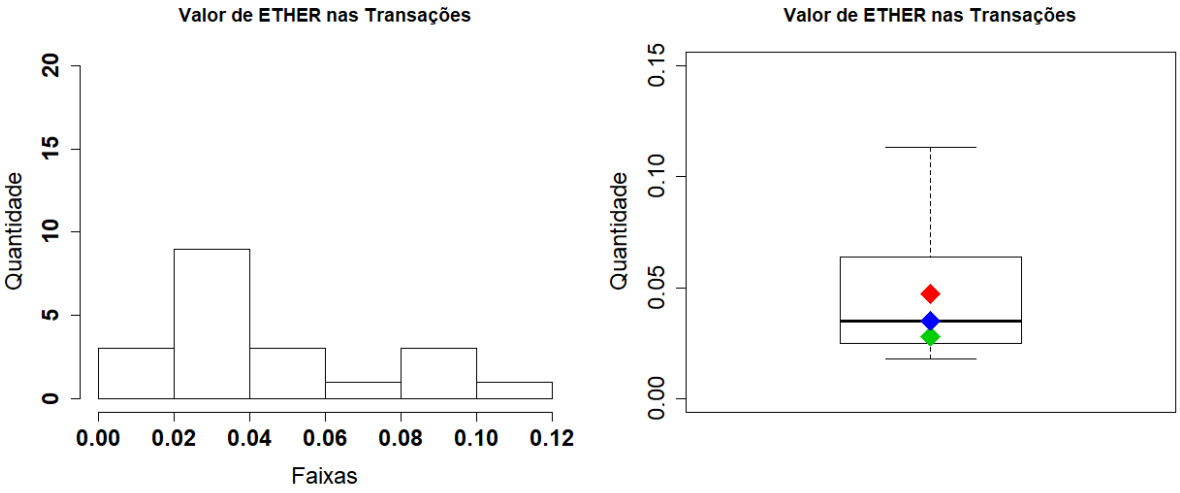
5.3.5 Atualização de Diplomas

A Figura 38 exibe o histograma e *boxplot* para os valores de *ether* coletados da funcionalidade atualizar diploma. O menor valor coletado foi 0,0177 e o maior foi 0,1131, ou seja, os valores de *ether* gastos nesse tipo de transação estão entre esse intervalo. A mediana foi 0,0351 *ether*, ou seja, metade das transações ocorreram com um valor menor que 0,0351 *ether* e a outra metade ocorreram com valor maior que 0,0351 *ether*. O primeiro quartil do *boxplot* tem o valor de 0,0258 *ether*, ou seja, um quarto das transações foram com um valor menor que 0,0258 *ether*. Já o terceiro quartil do *boxplot* tem valor de 0,0604 *ether*, ou seja, 75% das transações ocorreram com valor menor que 0,0604 *ether*. Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (0,1131 - 0,0177) é de 0,0954 *ether*. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de *ether* gasto nas transações.

A Figura 39 exibe o histograma e *boxplot* para os valores de *gas* coletados da funcionalidade atualizar diploma. O menor valor coletado foi 299670 e o maior foi 1185030, ou seja, os valores de *gas* gastos nesse tipo de transação estão entre esse intervalo. A mediana foi 600554 *gas*, ou seja, metade das transações ocorreram com um valor menor que 600554 *gas* e a outra metade ocorreram com valor maior que 600554 *gas*. O primeiro quartil do *boxplot* tem o valor de 415543 *gas*, ou seja, um quarto das transações foram com um valor menor que 415543 *gas*. Já o terceiro quartil do *boxplot* tem valor de 856342 *gas*, ou seja, 75% das transações ocorreram com valor menor que 856342 *gas*.

Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (1185030 - 299670) é de 885360 *gas*. No histograma também é possível visualizar

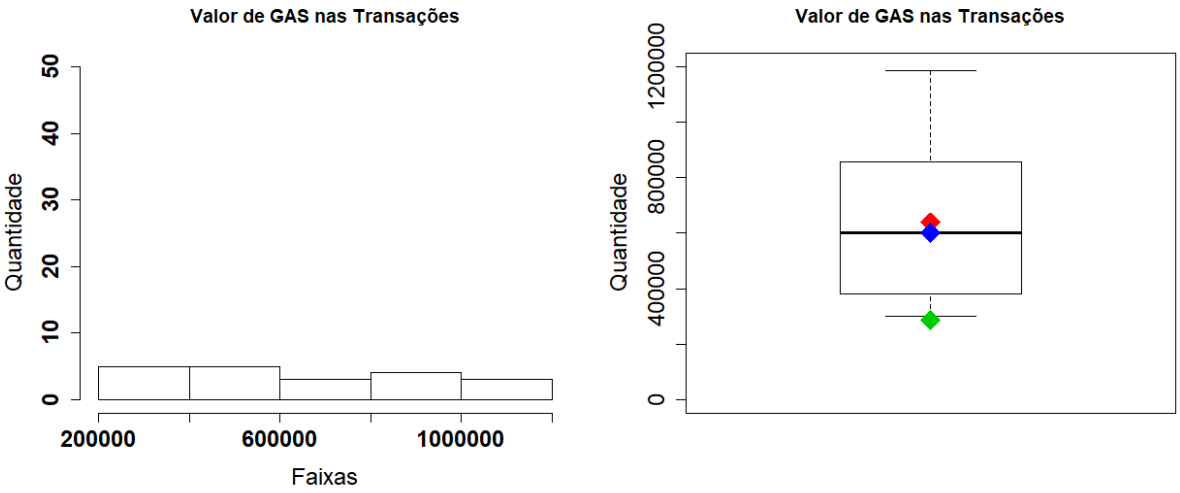
Figura 38 – Histograma e *boxplot* para valores coletados de *ether* da funcionalidade de atualização de diplomas



Fonte: Elaborada pelo autor.

as quantidades desse tipo de transação que foram realizadas por intervalo do valor de *gas* gasto nas transações.

Figura 39 – Histograma e *boxplot* para valores coletados de *gas* da funcionalidade de atualização de diplomas

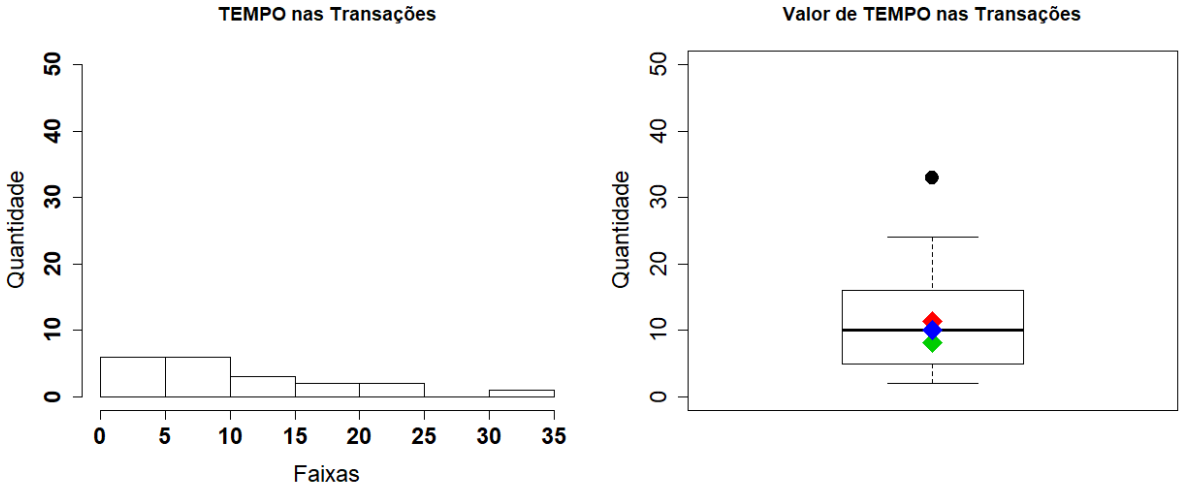


Fonte: Elaborada pelo autor.

A Figura 40 exibe o histograma e *boxplot* para os valores de tempo coletados da funcionalidade atualizar diploma. Na execução dessa funcionalidade também percebeu-se uma variabilidade de tempo considerável, e a ocorrência de um *outlier* (transação com tempo de 33 segundos), que apresentam um afastamento dos demais valores. Esse *outlier* identificado foram também uma transação executada em um momento que a rede Ethereum estava com instabilidades em seu ambiente. O menor tempo coletado foi 2 segundos e o maior foi 33

segundos, ou seja, os valores de tempo nesse tipo de transação estão entre esse intervalo. A mediana foi 10 segundos, ou seja, metade das transações ocorreram com um tempo menor que 10 segundos e a outra metade ocorreram com tempo maior que 10 segundos. O primeiro quartil do *boxplot* tem o tempo de 5 segundos, ou seja, um quarto das transações foram com um tempo menor que 5 segundos. Já o terceiro quartil do *boxplot* tem tempo de 15,50 segundos, ou seja, 75% das transações ocorreram com tempo menor que 15,50 segundos. Neste cenário, pode-se afirmar que o alcance da transação com maior tempo e a de menor tempo (33 - 2) é de 31 segundos. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de segundos gastos nas transações.

Figura 40 – Histograma e *boxplot* para valores coletados do tempo (segundos) para minerar o bloco da funcionalidade de atualização de diplomas



Fonte: Elaborada pelo autor.

A quantidade de transações executadas pelos participantes da avaliação nessa funcionalidade de atualizar diplomas foram 20 transações. A Tabela 7 apresenta um resumo dos valores estatísticos coletados da função atualizar diploma.

Tabela 7 – Valores estatísticos para a funcionalidade de atualização de diploma

Estatística	ETHER	GAS	TEMPO
Valor Mínimo	0,0177	299670	2,00
Valor Máximo	0,1131	1185030	33,00
Média	0,0471	638267	11,40
Mediana	0,0351	600554	10,00
Primeiro Quartil	0,0258	415543	5,00
Terceiro Quartil	0,0604	856342	15,50
Desvio Padrão	0,0281	286178,80	8,16

Fonte: o autor.

Os resultados obtidos são semelhantes a funcionalidade cadastrar diploma, pois essa função de atualizar trata-se de uma execução específica da função cadastrar para corrigir um diploma. Com isso, pode-se observar também um crescimento de custos de *ether* e *gas* baseado na quantidade e tamanho dos dados usado na transação. De forma semelhante ao cadastrar, existe também uma variação inconstante do tempo para minerar os blocos das transações. Considerando os valores mínimo, média e máximo de *ether* informados na Tabela 7, os mesmos representam R$ 40,53, R$ 107,85 e R$ 258,99 respectivamente.

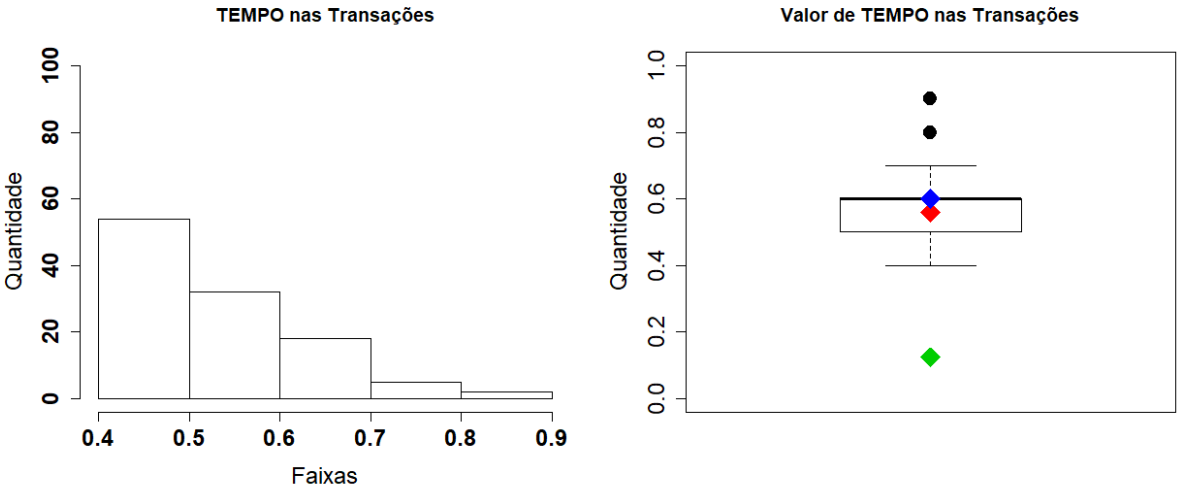
5.3.6 Consulta de Diplomas

A Figura 41 exibe o histograma e *boxplot* para os valores de tempo coletados da funcionalidade de consulta de diploma. Todas as execuções dessa funcionalidade tiveram tempo com menos de 1 segundo. Houve a ocorrência de dois *outliers* (consultas com tempo de 0,80 e 0,90 segundos). Esses *outliers* identificados foram consultas realizadas em momentos que a rede Ethereum estava com instabilidades em seu ambiente. O menor tempo coletado foi 0,40 segundos e o maior foi 0,90 segundos, ou seja, os valores de tempo das consultas estão entre esse intervalo. A mediana foi 0,60 segundos, ou seja, metade das consultas ocorreram com um tempo menor que 0,60 segundos e a outra metade ocorreram com tempo maior que 0,60 segundos. O primeiro quartil do *boxplot* tem o tempo de 0,50 segundos, ou seja, um quarto das consultas foram com um tempo menor que 0,50 segundos. Já o terceiro quartil do *boxplot* tem tempo de 0,60 segundos, ou seja, 75% das consultas ocorreram com tempo menor que 0,60 segundos. Neste cenário, pode-se afirmar que o alcance da consulta com maior tempo e a de menor tempo (0,90 - 0,40) é de 0,50 segundos. No histograma também é possível visualizar as quantidades de consultas que foram realizadas por intervalo do valor de segundos gastos nas consultas.

A quantidade de consultas realizadas foi 111, em que corresponde o número de CPF cadastros na aplicação pelos participantes da avaliação. A Tabela 8 apresenta um resumo dos valores estatísticos coletados da função consultar diploma.

Nessa função de consulta não existe custos associados a *ether* e *gas*, pois após as informações serem armazenadas na *blockchain* não é necessário utilizar *criptomoeda* para consultar as informações. Essas consultas são chamadas que apenas retornam os dados, ou seja, não realizam alteração nos dados armazenados na *blockchain*. Em relação as outras funcionalidades da aplicação elas realizam transações que inserem ou modificam os dados na *blockchain*, tendo um custo (*ether* e *gas*) associado que será cobrado no momento de executar as

Figura 41 – Histograma e *boxplot* para valores coletados do tempo (segundos) para minerar o bloco da funcionalidade de consulta de diplomas



Fonte: Elaborada pelo autor.

Tabela 8 – Valores estatísticos para a funcionalidade de consulta de diploma

Estatística	TEMPO
Valor Mínimo	0,40
Valor Máximo	0,90
Média	0,55
Mediana	0,60
Primeiro Quartil	0,50
Terceiro Quartil	0,60
Desvio Padrão	0,12

Fonte: o autor.

transações.

5.4 Análises e Discussão

O desenvolvimento de soluções baseadas em *blockchain* tem surgido cada vez mais no mercado e na academia. Existem diversas plataformas e ferramentas para se trabalhar com *blockchain* e nesse trabalho foram apresentadas algumas delas. A plataforma Ethereum se mostrou adequada para utilização nesse trabalho, devido ao conjunto de ferramentas identificadas que atende ao desenvolvimento da proposta. Além do vasto material didático de fácil acesso na internet ainda existe vários canais de suporte para resolver problemas e dúvidas do processo de desenvolvimento e utilização das ferramentas.

O questionário *online* aplicado aos especialistas no domínio de certificados refletiu

uma visão geral da percepção e entendimento da solução proposta. Pelo perfil das pessoas que participaram da pesquisa, a maioria tem um tempo considerável de experiência na área de educação e certificados. Existe uma diversidade considerável na área de atuação dos participantes, isso enriqueceu o *feedback* sobre o uso da aplicação proposta.

De acordo com as respostas da questão QD8, alguns participantes trabalham em uma IES que existe uma consulta para verificar os dados do diploma. Com isso, foi possível ter uma opinião mais clara em relação a comparação de uma solução tradicional e uma baseada em *blockchain*. A maioria dos participantes tinha conhecimento da portaria 1.095 do MEC antes da realização dessa pesquisa e também a maioria tinha conhecimento entre básico e intermediário sobre a tecnologia *blockchain*, facilitando o entendimento da pesquisa e o *feedback* dos participantes. De acordo com as respostas das questões QA1 e QA2, a maioria dos participantes afirmou que a aplicação foi de fácil utilização e navegação, mostrando uma experiência satisfatória por parte dos participantes durante a avaliação.

Através das respostas da questão QO1, pode-se destacar alguns benefícios para as IES com a proposta desse trabalho: (i) possibilidade de manter os dados distribuídos; (ii) alta disponibilidade da aplicação; e (iii) possibilidade de não precisar de uma infraestrutura local para manter aplicação.

Existem também benefícios relacionados diretamente com o dia a dia dos processos envolvendo diplomas nas IES: (i) possibilidade de diminuir os riscos de perda das informações; (ii) economizar papel; (iii) reduzir custos administrativos para realizar uma verificação de validade do diploma; e (iv) impedir documentos falsificados;

A extensão MetaMask foi citada como ponto franco da aplicação em algumas respostas das questões QO2 e QO3, devido a necessidade da confirmação das transações por ele antes de serem executadas. Essa extensão foi definida como pré-requisito para utilização da aplicação, pois como se trata de uma solução baseada em *blockchain* é necessário utilizar uma carteira de *criptomoeda* para executar as transações. Porém, o MetaMask é usado somente para executar transações que inserem ou alteram dados na *blockchain*, com isso, a função consultar diploma não precisa dessa extensão. Dessa forma, qualquer entidade pode consultar sem a necessidade da instalação da extensão como pré-requisito para validar os dados do diploma.

Em relação a análise de desempenho, a variável tempo para minerar os blocos das transações se mostrou inconstante em todas funcionalidades da aplicação, ou seja, observa-se uma quebra de padrão de crescimento do tempo baseado no tamanho dos dados usados nas

transações. Isso indica que mesmo utilizando dados com mesmo tamanho e formato em uma transação, o tempo para minerar os blocos podem ser bem distintos em execuções em momentos diferentes. Esse comportamento ocorre em todas funcionalidades da aplicação.

Na função cadastrar diploma a média geral das transações ficou em 13,95 segundos, tendo algumas transações executadas em até 2 segundos. Na função revogar diploma a média de tempo das transações ficou em 9,69 segundos, tendo algumas transações executadas em até 1 segundo. Na função atualizar diploma a média de tempo das transações ficou em 11,4 segundos, tendo algumas transações executadas em até 2 segundos. Na função consultar diploma a média de tempo das transações ficou em 0,55 segundos, tendo algumas transações executadas em até 0,4 segundos. Como pode-se observar, esse elevado tempo de espera para executar algumas transações pode ser um problema para o usuário final da aplicação, porém conforme respostas obtidas nas questões QA3 e QA4 do questionário aplicado para os especialistas no domínio de diplomas, o tempo de espera foi considerado satisfatório para todos participantes.

As variáveis *ether* e *gas* que representam os custos das transações tiveram um comportamento estável em todas funcionalidades da aplicação de acordo com a análise de desempenho, ou seja, a relação do crescimento dos custos baseado na quantidade e tamanho dos dados utilizados nas transações. Quanto maior a quantidade e tamanho dos dados para armazenar na *blockchain*, maior são os custos associados. Um destaque importante, foi a percepção da variação do valor de *Gwei* informados nas transações. Cada participante da avaliação informou um valor de *Gwei* diferente para executar suas transações. Os valores de *Gwei* informados considerando da primeira a última avaliação foram respectivamente 65, 58, 63, 110, 59, 105, 78, 67, 97 e 95. Esses valores foram colerados do ambiente real da Ethereum, com isso, é observada uma variação significativa do valor da *criptomoeda* no ambiente principal dessa plataforma em um curto espaço de tempo. Pelos valores de *Gwei* informados, percebe-se também que estavam altas as taxas para pagar financeiramente pelas transações durante o período da avaliação, por isso, algumas transações tiveram o valor em *ether* considerável para executar uma transação. Durante os testes realizados na fase de desenvolvimento da solução foram observados valores de *Gwei* menores que 30, que consequentemente estava gerando taxas menores para executar as transações. No questionário aplicado para os especialistas, houve resposta na questão QO2 que destaca a preocupação em avaliar os custos em *criptomoeda* das transações antes de adotar uma solução baseada em *blockchain*.

Em relação aplicação criada, destaca-se que ela foi implantada e utilizada na rede

Ropsten, que é uma rede de testes pública da Ethereum, que utiliza *criptomoeda* "falsa" para possibilitar testes de aplicações. Nesse tipo de rede existem algumas instabilidades relacionadas a própria natureza desse ambiente, pois se trata de uma infraestrutura para experimentos. Utilizando uma rede pública não foi preciso criar uma infraestrutura local para manter a *blockchain*, pois ela é mantida pelos próprios mineradores da rede Ethereum. Apesar dessa abordagem parecer benéfica por não ter custos associados para manter uma infraestrutura, existem os valores de taxas cobradas para executar as transações pelos mineradores da rede. Com isso, é importante observar os valores dessas taxas para realizar uma análise financeira caso a solução proposta seja implantada no ambiente real (principal) da Ethereum.

Uma segunda abordagem que não foi utilizada nesse trabalho, era a criação de uma instância privada (rede local) da Ethereum, onde é possível criar configurações específicas para determinar o número de nós na rede para validar os blocos criados e ter mais controle sobre a dificuldade de gerar novos blocos. Nessa abordagem o problema de custos associados as taxas cobradas pelos mineradores da rede pública pode ser resolvido, porém existem custos associados para criar e manter uma infraestrutura com número de nós suficientes para garantir um desempenho satisfatório na execuções das transações na rede *blockchain*. Com isso, é importante analisar também os custos associados a infraestrutura, no caso de implantações de soluções na rede principal da Ethereum.

Todas as etapas planejadas foram seguidas e desenvolvidas para criação de cada camada do modelo de arquitetura proposta neste trabalho, assim foi possível criar uma abordagem baseada em *blockchain* como uma solução para publicação em uma aplicação *web* de extratos de informações de certificados de alunos do ensino superior. Diante dos resultados obtidos, a proposta se mostrou adequada do ponto de vista funcional ao processo de armazenar e consultar dados de diplomas.

6 CONCLUSÃO

Uma grande variedade de aplicações está surgindo rapidamente com a tecnologia *blockchain*, porém no campo da educação ela está em estágio inicial, em que várias organizações da indústria e academia buscam os benefícios dessa tecnologia para área da educação.

De acordo com os resultados apresentados no cenário de avaliação, a abordagem proposta baseada na tecnologia *blockchain* poderia fornecer uma alternativa viável para armazenar e ter controle de acesso aos dados de certificados de alunos, pois utiliza uma plataforma segura para compartilhar dados e aumentar a confiança e a transparência na consulta da veracidade das informados dos diplomas dos estudantes.

O uso da tecnologia *blockchain* tem seus próprios desafios. Ao avaliar a praticidade de uma solução baseada em *blockchain*, os profissionais precisam cuidadosamente analisar a viabilidade das soluções capazes de atender a diferentes requisitos de negócios. Por isso, a crescente exploração dos potenciais para o uso de *blockchain*.

As principais vantagens da solução proposta foram: ajudar terceiros a verificar os registros dos diplomas, distribuir dados em vários locais, reduzindo a possibilidade de perder a informação e ter elevada disponibilidade para consulta ao diploma, uma vez que um nó da rede cair ou deixar de existir não impede que a informação esteja disponível para acesso.

6.1 Considerações Finais

Neste trabalho foi proposto um modelo de arquitetura utilizando a tecnologia *blockchain*, no qual foi desenvolvida uma aplicação para fornecer uma consulta aos dados dos diplomas dos alunos para todas as partes interessadas. O objetivo geral deste trabalho foi fornecer um ambiente através da tecnologia *blockchain* para publicar de forma *web* extrato das informações de diplomas de alunos do ensino superior. Para criação do ambiente foi montada uma infraestrutura que atendesse as necessidades da proposta, assim como um cenário de avaliação para alguns profissionais da área educacional. Por fim, foi realizado um estudo de análise de desempenho da aplicação criada.

A implementação da arquitetura de referência possibilita uma padronização para o desenvolvimento de aplicações que integram serviços diversos, de várias tecnologias (*web*, *mobile*, microsserviços, etc), com *blockchain*. Assim, os benefícios do uso de *blockchain* podem ser compartilhados para diversos serviços. Uma das ideias da arquitetura de referência é

identificar as camadas mais comumente utilizadas, organizá-las para uma melhor compreensão e facilitar o uso, instanciando ela para aplicações.

Neste contexto, foi abordado um problema relevante e oportuno ao propor e instanciar uma arquitetura de referência que aproveita a tecnologia moderna *blockchain*. Com o desenvolvimento e a experiência adquirida nesta pesquisa, buscou-se responder algumas questões de pesquisa relevantes.

Considerando a primeira questão elencada no trabalho "*Quais os principais desafios tecnológicos que as instituições educacionais podem enfrentar para inovar na área de gestão dos dados dos diplomas utilizando a tecnologia blockchain?*", destaca-se através do aprendizado adquirido ao longo da pesquisa e as percepções dos participantes da avaliação que as IES precisam adaptar alguns dos seus processos internos para se adequar a realidade em torno do domínio das *criptomoedas*, principalmente na gestão contábil das próprias IES, ou seja, como seria realizada a gestão financeira e a contabilidade dos gastos relacionados as *criptomoedas*. Complementar a isso, seria necessário avaliar o amparo legal no Brasil para realizar procedimentos (transações) envolvendo *criptomoedas*. Também aprendeu-se que é importante ter uma visão integrada das tecnologias tradicionais e a nova tecnologia para elaborar soluções que atendam os mais diversos requisitos de negócio. Com isso, é necessário profissionais capacitados com essa visão para desenvolver soluções que atendam de maneira satisfatória a realidade de cada IES.

Analisando a segunda questão de pesquisa "*É possível criar uma solução baseada em blockchain para atender os requisitos da portaria de número 1.095 do MEC, que exige a publicação de um extrato das informações sobre os registros realizados no DOU?*", destacam-se as respostas da questão QA5 do questionário aplicado, em que todos os participantes apontam que é possível criar uma solução baseada nessa tecnologia. Dessa forma, acredita-se que a tecnologia *blockchain* tem potencial para atender os requisitos da portaria 1.095 para manter um banco de informações de registro de diplomas de forma *web*, após realizado o devido registro no DOU.

Avaliando a terceira e última questão de pesquisa foi "*Existem diferenças significativas do ponto de vista do usuário final entre uma solução baseada em blockchain e uma solução tradicional para manter um banco de informações de registro de diplomas a ser disponibilizado na web, após realizado o devido registro dos diplomas no DOU?*". Para responder a essa indagação, destacam-se as respostas da questão QA6 do questionário aplicado, em que a maioria dos participantes apontaram que não existem diferenças significativas. Os participantes

tiveram a oportunidade de validar a aplicação Web desenvolvida, que utiliza uma *blockchain* de forma transparente para armazenar os dados dos diplomas. Cada participante baseado nas suas experiências, analisou as possíveis diferenças entre as tecnologias tradicionais e a tecnologia *blockchain*. Essa questão de pesquisa tenta avaliar a percepção das pessoas em relação ao uso de *blockchain*, pois essa tecnologia é geralmente relacionada ao mercado financeiro e pouco apresentada as outras áreas do mercado, como por exemplo, educação. Geralmente, existe também a visão que para o usuário comum (não desenvolvedor) usar uma solução com *blockchain* é necessário ter um poder computacional considerável, ter conhecimento considerável em TI ou até mesmo ter conhecimento considerável em *blockchain*, no entanto, a solução proposta nesse trabalho foi considerada simples de uma forma geral pelos participantes da avaliação. Requisitos como esses geralmente não ocorrem para usar uma solução com tecnologia tradicional para disponibilizar um banco de informações de registro de diplomas de forma *web*, pois geralmente as pessoas bastam acessar o endereço na *web* e seguir um passo a passo para utilizar as funções de uma determinada aplicação.

6.2 Publicações

Alguns artigos foram submetidos com resultados desta pesquisa e trabalhos relacionados. O Quadro 2 lista os artigos publicados, tanto em conferências como em periódicos.

Quadro 2 – Artigos publicados em conferências e periódicos

Artigo	**Veículo de Publicação**
A Pattern Adherence Analysis to a Blockchain Web Application	IEEE International Conference on Software Architecture Companion (BlockArch-ICSAC 2020)
Towards Cloud Computing and Blockchain Integrated Applications	IEEE International Conference on Software Architecture Companion (BlockArch-ICSAC 2020)
Motivating Web and Blockchain Application Modeling	IEEE International Conference on Software Architecture Companion (BlockArch-ICSAC 2020)
Avaliando o Custo de Contratos Inteligentes em Aplicações Blockchain por meio de Ambientes de Simulação	II Workshop de Modelagem e Simulação de sistemas intensivos em Software (MSSiS 2020)
A Blockchain-based Architecture for Query and Registration of Student Degree Certificates	XIV Simpósio Brasileiro de Componentes, Arquiteturas e Reutilização de Software (SBCARS 2020)
Modeling Blockchain E-health Systems	10th Euro American Conference on Telematics and Information Systems (EATIS 2020)
Oportunidades de Pesquisa em Blockchain em Tempos de Pandemia	Revista Sistemas e Mídias Digitais (RSMD)
Aplicando Blockchain sobre Dados Educacionais	Revista Sistemas e Mídias Digitais (RSMD)

Fonte: elaborado pelo autor.

6.3 Limitações do Trabalho

Neste trabalho algumas limitações da pesquisa puderam ser identificadas, descritas a seguir. Também procurou-se descrever uma forma de como mitigá-las.

A avaliação do protótipo construído foi realizada em uma *blockchain* pública de testes devido à falta de tempo e capital financeiro para custear despesas com a compra de *criptomoeda* real para realizar a avaliação da aplicação na rede principal da Ethereum. O ambiente de testes é semelhante ao principal, sendo que o principal impacto na mudança de um para o outro é a necessidade de um investimento financeiro em *criptomoeda* para executar as transações. Com isso, é interessante um estudo de custos financeiros com *criptomoeda* no ambiente real da Ethereum para utilizar a aplicação proposta para comparar com os custos para desenvolver e manter uma aplicação utilizando tecnologias tradicionais. Assim ficaria mais claro qual modelo de negócio é mais vantajoso para as instituições manter um banco de informações de registro de diplomas de forma *web*.

Outro ponto importante é a necessidade de avaliar as leis do país em questão sobre aplicações com *blockchain*, pois ela é uma rede descentralizada e pode enfrentar dificuldades legais para armazenar e fornecer de forma distribuída consultas aos dados de instituições e estudantes. Com isso, é interessante realizar uma pesquisa no domínio jurídico direcionada para uso de *criptomoedas* para armazenar informações de pessoas e organizações, a fim de esclarecer questões legais relacionadas a privacidade dos dados.

A pesquisa utilizou um questionário com questões de múltipla escolha e abertas para avaliação com especialistas. Há a possibilidade de alguns problemas no preenchimento. Uma situação é a não compreensão das questões. Outra é a possibilidade de algumas pessoas ainda estarem em processo de aprendizagem no domínio educacional. Por fim, as respostas foram de uma mesma região, cidades do Estado do Ceará, e com apenas 5 instituições educacionais. Com isso, seria interessante realizar uma avaliação com mais instituições, de preferência com a presença de algum profissional do MEC para representar o governo brasileiro durante a avaliação.

Em relação a aplicação desenvolvida, poucos cenários foram analisados, sendo interessante avaliar outras funcionalidades além de cadastrar, revogar, atualizar e consultar diplomas. Algumas situações como o desenvolvimento de relatórios e integrações com sistemas tradicionais foram citadas na avaliação pelos participantes, em que podem ser pontos importantes para entregar uma solução satisfatória para o usuário final.

Por fim, embora exista a evolução das ferramentas e infraestrutura da *blockchain*

Ethereum, as bibliotecas ainda estão em fase de desenvolvimento para suportar a maioria das necessidades dos desenvolvedores e organizações do mercado e academia.

6.4 Trabalhos Futuros

Esta pesquisa promoveu a possibilidade de diversos trabalhos futuros, seja do ponto de vista tecnológico, de aplicação e de negócio.

Pretende-se realizar um estudo de caso na rede principal da Ethereum para avaliar a performance da aplicação em relação aos custos e tempo das transações nesse ambiente. Também pretende-se avaliar a proposta com outras instituições educacionais com a presença de algum profissional do MEC para representar a entidade governo. Considerando também a avaliação dos aspectos legais para implantação da solução em ambiente real.

Outro trabalho futuro é avaliar novas ferramentas a fim de analisar e desenvolver as melhorias sugeridas pelos participantes da avaliação. Destacam-se melhorias como geração de relatórios para controle gerencial das informações. Também buscar formas de integração com sistemas tradicionais do mercado para facilitar a exportação de informações para sistemas baseados em *blockchain*, sendo que o caso contrário também é interessante, pois o cruzamento de informações entre sistemas diferentes é um típico mecanismo usado pelas instituições para ter um melhor controle das informações geradas.

Ampliar as funcionalidades implicam em testes. Existem diversos tipos de testes (unitário, integração, sistêmico, desempenho, etc), e um trabalho com aspectos em arquitetura e interoperabilidade possui uma demanda grande para testes em software.

Avaliar outras plataformas de *blockchain*, como o Hyperledger, é uma opção interessante de trabalho futuro. O Hyperledger possui uma grande comunidade de usuários e ferramentas que podem colaborar para a implantação da solução de certificados, além de ser uma alternativa a Ethereum.

Do ponto de vista de funcionalidades, cada uma das quatro funções básicas (cadastrar, revogar, atualizar e consultar) podem ser ampliadas. Diversas melhorias foram sugeridas na pesquisa, seja de novas funcionalidades ou interface do usuário.

Analisando sob a visão de modelagem, alguns modelos podem apoiar o desenvolvimento de soluções em *blockchain*. Abreu e Coutinho (2020) iniciaram uma breve motivação sobre a importância de modelagem entre sistemas *web* e *blockchain*. Uma ideia é expandir com modelos estáticos, como diagramas de classes, dinâmicos e de sequência. Outra oportunidade é a

aplicação de padrões, como os descritos por Xu *et al.* (2018), que são específicos para *blockchain*. Como parte do trabalho envolve a comunicação entre dados internos e externos a *blockchain*, alguns padrões de projeto para esse fim foram desenvolvidos, e podem ser estudados para refinar os modelos das aplicações.

Ainda sobre modelagem, uma oportunidade seria modelar a utilização da aplicação desenvolvida utilizando *Business Process Model and Notation* (BPMN). Essa opção se deve ao fato do BPMN descrever a lógica de um processo de negócio por meio de diagramas de maneira simples e direta. Assim, os requisitos da aplicação podem ser modelados mais claramente.

Há também a necessidade de se avaliar a qualidade de aplicações *blockchain*. Uma oportunidade seria explorar o trabalho de Ciccio *et al.* (2020), onde critérios e perspectivas de qualidade para o modelo de negócio de aplicações *blockchain* são apresentados. A tendência seria analisar requisitos não funcionais, a infraestrutura, usabilidade e regras de negócio para a aplicação.

Por fim, estender os recursos da aplicação criada e analisar como tornar a aplicação mais aderente aos processos envolvendo os diplomas dos estudantes.

REFERÊNCIAS

ABREU, A. W.; COUTINHO, E. F. Motivating web and blockchain application modeling. In: **2020 IEEE International Conference on Software Architecture Companion (ICSA-C)**. New York, NY, USA: IEEE, 2020. p. 110–113. Disponível em: https://ieeexplore.ieee.org/document/9095632. Acesso em: 20 nov. 2020.

ALAMMARY, A.; ALHAZMI, S.; ALMASRI, M.; GILLANI, S. Blockchain-based applications in education: A systematic review. **Applied Sciences**, Multidisciplinary Digital Publishing Institute, v. 9, n. 12, p. 2400, 2019.

ALBERT, E.; CORREAS, J.; GORDILLO, P.; ROMÁN-DÍEZ, G.; RUBIO, A. Gasol: Gas analysis and optimization for ethereum smart contracts. In: BIERE, A.; PARKER, D. (Ed.). **Tools and Algorithms for the Construction and Analysis of Systems**. Cham: Springer International Publishing, 2020. p. 118–125. ISBN 978-3-030-45237-7.

ALHARBY, M.; MOORSEL, A. van. Blockchain-based smart contracts: A systematic mapping study. **arXiv preprint arXiv:1710.06372**, 2017.

ANDROULAKI, E.; BARGER, A.; BORTNIKOV, V.; CACHIN, C.; CHRISTIDIS, K.; CARO, A. D.; ENYEART, D.; FERRIS, C.; LAVENTMAN, G.; MANEVICH, Y.; MURALIDHARAN, S.; MURTHY, C.; NGUYEN, B.; SETHI, M.; SINGH, G.; SMITH, K.; SORNIOTTI, A.; STATHAKOPOULOU, C.; VUKOLIć, M.; COCCO, S. W.; YELLICK, J. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: **Proceedings of the Thirteenth EuroSys Conference**. New York, NY, USA: Association for Computing Machinery, 2018. (EuroSys '18). ISBN 9781450355841. Disponível em: https://doi.org/10.1145/3190508.3190538. Acesso em: 22 set. 2020

AZARIA, A.; EKBLAW, A.; VIEIRA, T.; LIPPMAN, A. Medrec: Using blockchain for medical data access and permission management. In: **2016 2nd International Conference on Open and Big Data (OBD)**. New York, NY, USA: IEEE, 2016. p. 25–30.

BACH, L. M.; MIHALJEVIC, B.; ZAGAR, M. Comparative analysis of blockchain consensus algorithms. In: **2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)**. New York, NY, USA: IEEE, 2018. p. 1545–1550.

BANASIK, W.; DZIEMBOWSKI, S.; MALINOWSKI, D. Efficient zero-knowledge contingent payments in cryptocurrencies without scripts. In: ASKOXYLAKIS, I.; IOANNIDIS, S.; KATSIKAS, S.; MEADOWS, C. (Ed.). **Computer Security – ESORICS 2016**. Cham: Springer International Publishing, 2016. p. 261–280.

BASHIR, I. **Mastering blockchain**. Birmingham, UK: Packt Publishing Ltd, 2017. 198–201 p. ISBN 9781787125445.

BEDI, P.; GOLE, P.; DHIMAN, S.; GUPTA, N. Smart contract based central sector scheme of scholarship for college and university students. **Procedia Computer Science**, v. 171, p. 790 – 799, 2020. ISSN 1877-0509. Third International Conference on Computing and Network Communications (CoCoNet'19). Disponível em: http://www.sciencedirect.com/science/article/pii/S1877050920310553. Acesso em: 22 set. 2020.

BHASKAR, N. D.; CHUEN, D. L. K. Bitcoin mining technology. In: CHUEN, D. L. K. (Ed.). **Handbook of Digital Currency**. San Diego: Academic Press, 2015. cap. 3, p. 45–65.

BOSU, A.; IQBAL, A.; SHAHRIYAR, R.; CHAKRABORTY, P. Understanding the motivations, challenges and needs of blockchain software developers: A survey. **Empirical Software Engineering**, Springer, v. 24, n. 4, p. 2636–2673, 2019. ISSN 1573-7616. Disponível em: https://doi.org/10.1007/s10664-019-09708-7. Acesso em: 20 nov. 2020.

BRASIL. **Portaria nº 1095, de 25 de outubro de 2018. Expedição e registro de diplomas de cursos superiores de graduação no âmbito do sistema federal de ensino**. 2018. Diário Oficial da União, Brasília, DF, n. 207, p. 32, 26 out. 2018. Seção I. Disponível em: http://abmes.org.br/arquivos/legislacoes/Port-MEC-1095-2018-10-25.pdf. Acesso em: 20 nov. 2020.

CHENG, J.-C.; LEE, N.-Y.; CHI, C.; CHEN, Y.-H. Blockchain and smart contract for digital certificate. In: **2018 IEEE International Conference on Applied System Invention (ICASI)**. [*S. l.*: *s. n.*], 2018. p. 1046–1051.

CHOHAN, U. W. The double spending problem and cryptocurrencies. **SSRN**, p. 1–8, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174. Acesso em: 20 nov. 2020.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. **IEEE Access**, v. 4, p. 2292–2303, 2016.

CICCIO, C. D.; MERONI, G.; PLEBANI, P. Business process monitoring on blockchains: Potentials and challenges. In: NURCAN, S.; REINHARTZ-BERGER, I.; SOFFER, P.; ZDRAVKOVIC, J. (Ed.). **Enterprise, Business-Process and Information Systems Modeling**. Cham: Springer International Publishing, 2020. p. 36–51. ISBN 978-3-030-49418-6.

DELAHUNTY, S. **Developments And Adoption Of Blockchain In The U.S. Federal Government**. 2018. Https://www.forbes.com/sites/forbestechcouncil/2018/01/25/developments-and-adoption-of-blockchain-in-the-u-s-federal-government/228d3c1b3d99. Acesso em: 20 nov. 2020.

DELMOLINO, K.; ARNETT, M.; KOSBA, A.; MILLER, A.; SHI, E. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In: CLARK, J.; MEIKLEJOHN, S.; RYAN, P. Y.; WALLACH, D.; BRENNER, M.; ROHLOFF, K. (Ed.). **Financial Cryptography and Data Security**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016. p. 79–94. ISBN 978-3-662-53357-4.

DENCKER, J. C. Outliers: The story of success. **Academy of Management Perspectives**, v. 24, n. 3, p. 97–99, 2010. Disponível em: https://doi.org/10.5465/amp.24.3.97. Acesso em: 20 nov. 2020.

DUAN, B.; ZHONG, Y.; LIU, D. Education application of blockchain technology: Learning outcome and meta-diploma. In: **2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)**. New York, NY, USA: IEEE, 2017. p. 814–817. ISSN 1521-9097.

EGBERTSEN, W.; HARDEMAN, G.; HOVEN, M. van den; KOLK, G. van der; RIJSEWIJK, A. van. **Replacing Paper Contracts With Ethereum Smart Contracts**. 2016. Disponível em: https://allquantor.at/blockchainbib/pdf/egbertsen2016replacing.pdf. Acesso em: 2 nov. 2020.

EVERLEDGER. **A Digital Global Ledger**. 2018. Https://www.everledger.io/. Acesso em: 20 nov. 2020.

GATTESCHI, V.; LAMBERTI, F.; DEMARTINI, C.; PRANTEDA, C.; SANTAMARíA, V. Blockchain and smart contracts for insurance: Is the technology mature enough? **Future Internet**, v. 10, p. 20, 02 2018.

GHAFFAR, A.; HUSSAIN, M. Bceap - a blockchain embedded academic paradigm to augment legacy education through application. In: **Proceedings of the 3rd International Conference on Future Networks and Distributed Systems**. New York, NY, USA: Association for Computing Machinery, 2019. (ICFNDS '19). ISBN 9781450371636. Disponível em: https://doi.org/10.1145/3341325.3342036. Acesso em: 22 set. 2020.

GRECH, A.; CAMILLERI, A. F. **Blockchain in Education. JRC Science for Policy Report**. 2017. Https://goo.gl/gG4F1w. Acesso em: 20 nov. 2020.

GREVE, F.; SAMPAIO, L.; ABIJAUDE, J.; COUTINHO, A. A.; BRITO, I.; QUEIROZ, S. Blockchain e a revolução do consenso sob demanda. In: **Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. Porto Alegre, RS: Sociedade Brasileira de Computação, 2018.

HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. In: MENEZES, A. J.; VANSTONE, S. A. (Ed.). **Advances in Cryptology-CRYPTO' 90**. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991. p. 437–455. ISBN 978-3-540-38424-3.

HAN, M.; LI, Z.; HE, J. S.; WU, D.; XIE, Y.; BABA, A. A novel blockchain-based education records verification solution. I n: **Proceedings of the 19th Annual SIG Conference on Information Technology Education**. New York, NY, USA: Association for Computing Machinery, 2018. (SIGITE '18), p. 178–183. ISBN 9781450359542. Disponível em: https://doi.org/10.1145/3241815.3241870. Acesso em: 22 set. 2020.

HARTHY, K. A.; SHUHAIMI, F. A.; ISMAILY, K. K. J. A. The upcoming blockchain adoption in higher-education: requirements and process. In: **2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)**. New York, NY, USA: IEEE, 2019. p. 1–5.

HUH, S.; CHO, S.; KIM, S. Managing iot devices using blockchain platform. In: **2017 19th International Conference on Advanced Communication Technology (ICACT)**. New York, NY, USA: IEEE, 2017. p. 464–467.

ISHMAEV, G. Blockchain technology as an institution of property. **Metaphilosophy**, v. 48, n. 5, p. 666–686, 2017. 2020. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/meta.12277. Acesso em: 20 nov.

ISLAM, I.; MUNIM, K. M.; OISHWEE, S. J.; ISLAM, A. K. M. N.; ISLAM, M. N. A critical review of concepts, benefits, and pitfalls of blockchain technology using concept map. **IEEE Access**, v. 8, p. 68333–68341, 2020. ISSN 2169-3536.

IVAKI, N.; LARANJEIRO, N.; ARAUJO, F. A survey on reliable distributed communication. **Journal of Systems and Software**, v. 137, p. 713–732, 2018. ISSN 0164-1212.Disponível em: http://www.sciencedirect.com/science/article/pii/S0164121217300651. Acesso em: 20 nov. 2020.

JAIN, R. **The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling**. 1st. ed. [*S. l.*]: John Wiley and Sons, INC, 1991. 685 p. ISBN 1-471-50336-3.

KAMIŠALIĆ, A.; TURKANOVIĆ, M.; MRDOVIĆ, S.; HERIČKO, M. A preliminary review of blockchain-based solutions in higher education. In: UDEN, L.; LIBERONA, D.; SANCHEZ, G.; RODRÍGUEZ-GONZÁLEZ, S. (Ed.). **Learning Technology for Education Challenges**. Cham: Springer International Publishing, 2019. p. 114–124. ISBN 978-3-030-20798-4.

KANAN, T.; OBAIDAT, A. T.; AL-LAHHAM, M. Smartcert blockchain imperative for educational certificates. In: **2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)**. New York, NY, USA: IEEE, 2019. p. 629–633.

KITCHENHAM, B.; BRERETON, P. A systematic review of systematic review process research in software engineering. **Information and software technology**, Elsevier, v. 55, n. 12, p. 2049–2075, 2013.

KORPELA, K.; HALLIKAS, J.; DAHLBERG, T. Digital supply chain transformation toward blockchain integration. In: **50th Hawaii International Conference on System Sciences (HICSS)**. Honolulu, HI: ScholarSpace, 2017.

LU, Q.; XU, X.; LIU, Y.; ZHANG, W. Design pattern as a service for blockchain applications. In: **2018 IEEE International Conference on Data Mining Workshops (ICDMW)**. New York, NY, USA: IEEE, 2018. p. 128–135. ISSN 2375-9259.

MEC. **Brazilian Ministry of Education - Higher Education Census**. 2019. Http://portal.mec.gov.br/component/content/article?id=80481. Acesso em: 20 mar. 2020.

MIGUEL, E. C. **Overlay construction strategies for peer-to-peer live streaming systems**. Tese (Doutorado) – Universidade Federal de Minas Gerais, 2017. Disponível em: http://hdl.handle.net/1843/JCES-AWVP4H. Acesso em: 20 nov. 2020.

NAKAGAWA, E. Y.; GUESSI, M.; MALDONADO, J. C.; FEITOSA, D.; OQUENDO, F. Consolidating a process for the design, representation, and evaluation of reference architectures. In: **2014 IEEE/IFIP Conference on Software Architecture**. New York, NY, USA: IEEE, 2014. p. 143–152.

NAKAGAWA, E. Y.; OQUENDO, F.; BECKER, M. Ramodel: A reference model for reference architectures. In: **2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture**. New York, NY, USA: IEEE, 2012. p. 297–301.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008.Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 20 nov. 2020.

NGUYEN, D.-H.; NGUYEN-DUC, D.-N.; HUYNH-TUONG, N.; PHAM, H.-A. Cvss: A blockchainized certificate verifying support system. In: **Proceedings of the Ninth International Symposium on Information and Communication Technology**. New York, NY, USA: Association for Computing Machinery, 2018. (SoICT 2018), p. 436–442. ISBN 9781450365390. Disponível em: https://doi.org/10.1145/3287921.3287968. Acesso em: 22 set. 2020.

NOFER, M.; GOMBER, P.; HINZ, O.; SCHIERECK, D. Blockchain. **Business & Information Systems Engineering**, v. 59, n. 3, p. 183–187, Jun 2017. ISSN 1867-0202. Disponível em: https://doi.org/10.1007/s12599-017-0467-3. Acesso em: 20 nov. 2020.

PEDERSEN, A. B.; RISIUS, M.; BECK, R. A ten-step decision path to determine when to use blockchain technologies. **MIS Quarterly Executive**, AIS Journals, v. 18, n. 2, 2019. Disponível em: https://aisel.aisnet.org/misqe/vol18/iss2/3. Acesso em: 02 nov. 2020.

POPOVIC, D.; AVIS, C.; BYRNE, M.; CHEUNG, C.; DONOVAN, M.; FLYNN, Y.; FOTHERGILL, C.; HOSSEINZADEH, Z.; LIM, Z.; SHAH, J.; AL. et. Understanding blockchain for insurance use cases. **British Actuarial Journal**, Cambridge University Press, v. 25, p. e13, 2020.

QIN, R.; YUAN, Y.; WANG, F. Research on the selection strategies of blockchain mining pools. **IEEE Transactions on Computational Social Systems**, v. 5, n. 3, p. 748–757, 2018. ISSN 2329-924X.

RIFI, N.; RACHKIDI, E.; AGOULMINE, N.; TAHER, N. C. Towards using blockchain technology for ehealth data access management. In: **2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)**. New York, NY, USA: IEEE, 2017. p. 1–4.

SECUREKEY. **Building Trusted Identity Networks**. 2017. Https://securekey.com/. Acesso em: 20 nov. 2020.

SERPRO. **Serpro desenvolve rede BlockChain para a Receita Federal**. 2019. Https://www.serpro.gov.br/menu/imprensa/Releases/serpro-desenvolve-rede-blockchain-para-a-receita-federal. Acesso em: 3 ago. 2020.

SHARPLES, M.; DOMINGUE, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In: VERBERT, K.; SHARPLES, M.; KLOBUČAR, T. (Ed.). **Adaptive and Adaptable Learning**. Cham: Springer International Publishing, 2016. p. 490–496. ISBN 978-3-319-45153-4.

SILLABER, C.; WALTL, B. Life cycle of smart contracts in blockchain ecosystems. **Datenschutz und Datensicherheit - DuD**, Springer, v. 41, n. 8, p. 497–500, Aug 2017. ISSN 1862-2607. Disponível em: https://doi.org/10.1007/s11623-017-0819-7. Acesso em: 20 nov. 2020.

SINGHAL, B.; DHAMEJA, G.; PANDA, P. S. How ethereum works. In: **Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions**. Berkeley, CA: Apress, 2018. p. 219–266. ISBN 978-1-4842-3444-0. Disponível em: https://doi.org/10.1007/978-1-4842-3444-0_4. Acesso em: 20 nov. 2020.

STEEN, M. v.; TANENBAUM, A. S. **Distributed Systems**. 3rd. ed. [*S. l.*]: CreateSpace Independent Publishing Platform, 2017. 7–20 p. ISBN 978–1543057386.

SZABO, N. **Smart Contracts**. 1994. Http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Acesso em: 20 nov. 2020.

TAUFIQ, R.; TRISETYARSO, A.; MEYLIANA; KOSALA, R.; RANTI, B.; SUPANGKAT, S.; ABDURACHMAN, E. Robust crypto-governance graduate document storage and fraud avoidance certificate in indonesian private university. In: **2019 International Conference on Information Management and Technology (ICIMTech)**. New York, NY, USA: IEEE, 2019. v. 1, p. 339–344.

THAKKAR, P.; NATHAN, S.; VISWANATHAN, B. Performance benchmarking and optimizing hyperledger fabric blockchain platform. In: **2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)**. New York, NY, USA: IEEE, 2018. p. 264–276. ISSN 1526-7539.

TURKANOVIć, M.; HöLBL, M.; KOšIč, K.; HERIčKO, M.; KAMIšALIć, A. Eductx: A blockchain-based higher education credit platform. **IEEE Access**, v. 6, p. 5112–5127, 2018. ISSN 2169-3536.

VIDAL, F.; GOUVEIA, F.; SOARES, C. Analysis of blockchain technology for higher education. In: **2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)**. New York, NY, USA: IEEE, 2019. p. 28–33.

VIDAL, F. R.; GOUVEIA, F.; SOARES, C. Revocation mechanisms for academic certificates stored on a blockchain. In: **2020 15th Iberian Conference on Information Systems and Technologies (CISTI)**. New York, NY, USA: IEEE, 2020. p. 1–6. ISSN 2166-0727.

WAN, Z.; XIA, X.; HASSAN, A. E. What is discussed about blockchain? a case study on the use of balanced lda and the reference architecture of a domain to capture online discussions about blockchain platforms across the stack exchange communities. **IEEE Transactions on Software Engineering**, p. 1–1, 2019. ISSN 1939-3520.

WANG, W.; HOANG, D. T.; HU, P.; XIONG, Z.; NIYATO, D.; WANG, P.; WEN, Y.; KIM, D. I. A survey on consensus mechanisms and mining strategy management in blockchain networks. **IEEE Access**, v. 7, p. 22328–22370, 2019. ISSN 2169-3536.

WHITE, M. **Digitizing Global Trade with Maersk and IBM**. 2018. Https://www.ibm.com/blogs/blockchain/2018/01/ digitizing-global-trade-maersk-ibm/. Acesso em: 20 nov. 2020.

WOOD, G. **Ethereum: A secure decentralised generalised transaction ledger**. 2019. Https://gavwood.com/paper.pdf. Acesso em: 20 nov. 2020.

XIAO, Y.; ZHANG, N.; LOU, W.; HOU, Y. T. A survey of distributed consensus protocols for blockchain networks. **IEEE Communications Surveys Tutorials**, v. 22, n. 2, p. 1432–1465, Secondquarter 2020. ISSN 1553-877X.

XU, X.; PAUTASSO, C.; ZHU, L.; LU, Q.; WEBER, I. A pattern collection for blockchain-based applications. In: **Proceedings of the 23rd European Conference on Pattern Languages of Programs**. New York, NY, USA: Association for Computing Machinery, 2018. (EuroPLoP '18). ISBN 9781450363877. Disponível em: https://doi.org/10.1145/3282308.3282312. Acesso em: 20 nov. 2020.

XU, X.; WEBER, I.; STAPLES, M. Blockchain in software architecture. In: ____. **Architecture for Blockchain Applications**. Cham: Springer International Publishing, 2019. p. 83–92. ISBN 978-3-030-03035-3. Disponível em: https://doi.org/10.1007/978-3-030-03035-3_5. Acesso em: 20 nov. 2020.

XU, X.; WEBER, I.; STAPLES, M.; ZHU, L.; BOSCH, J.; BASS, L.; PAUTASSO, C.; RIMBA, P. A taxonomy of blockchain-based systems for architecture design. In: **2017 IEEE International Conference on Software Architecture (ICSA)**. New York, NY, USA: IEEE, 2017. p. 243–252.

YEOH, P. Regulatory issues in blockchain technology. **Journal of Financial Regulation and Compliance**, Emerald Publishing Limited, v. 25, n. 2, p. 196–208, 2017. ISSN 1358-1988. Disponível em: https://doi.org/10.1108/JFRC-08-2016-0068. Acesso em: 20 nov. 2020.

ZOGBI, P. **Governo chileno vai usar blockchain do Ethereum na área de energia**. 2018. Https://www.infomoney.com.br/mercados/governo-chileno-vai-usar-blockchain-do-ethereum-na-area-de-energia/. Acesso em: 20 nov. 2020.

ZUO, X.; IAMNITCHI, A. A survey of socially aware peer-to-peer systems. **ACM Comput. Surv.**, Association for Computing Machinery, New York, NY, USA, v. 49, n. 1, maio 2016. ISSN 0360-0300. Disponível em: https://doi.org/10.1145/2894761. Acesso em: 20 nov. 2020.

APÊNDICE A – MANUAL DE INSTALAÇÃO DO METAMASK

Para utilizar aplicação Educ-Dapp é necessário a instalação da extensão MetaMask no navegador. Essa extensão representa uma carteira de *criptomoeda* para interagir com a rede Ethereum, em que aplicação foi baseada e criada. O MetaMask pode ser instalado nos navegadores Chrome, Firefox, Opera e Brave.

Para iniciar a instalação basta acessar o link <https://metamask.io/> e seguir os passos para instalar o MetaMask no navegador da sua preferência. Também é possível realizar a instalação através da loja de extensões do próprio navegador, em que basta pesquisar por MetaMask e seguir as orientações para instalação. A seguir, os detalhes dos passos para realizar a instalação.

A.1 Detalhes da Instalação

A Figura 42 mostra o passo inicial da instalação no navegador Chrome (nos outros navegadores os passos são semelhantes).

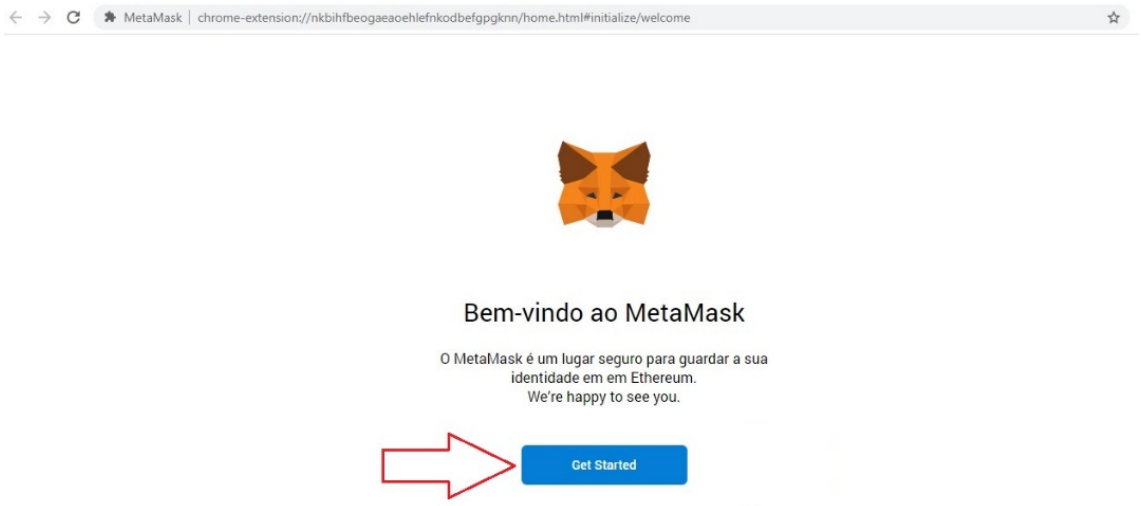


Figura 42 – Passo inicial instalação MetaMask.

Em seguida tem as opções de instalar com uma conta existente ou criar uma nova conta. Iremos criar uma nova conta para exemplificar o processo de instalação desde o princípio (Figura 43). Na etapa seguinte para prosseguir com a instalação é necessário aceitar os termo de uso do MetaMask (Figura 44). Na próxima etapa é necessário informar uma senha para acesso a conta do MetaMask. Após preencher, basta marcar que aceita os termos de uso e clicar em criar (Figura 45).

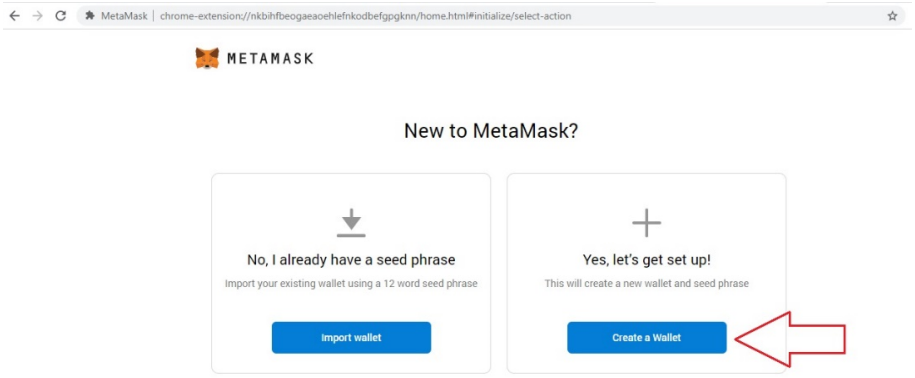


Figura 43 – Criar uma conta no MetaMask.

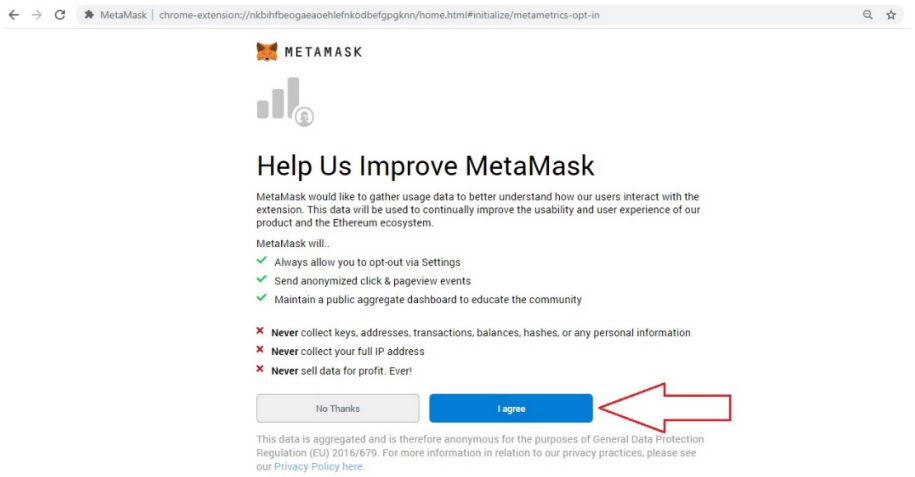


Figura 44 – Termos da conta do MetaMask.

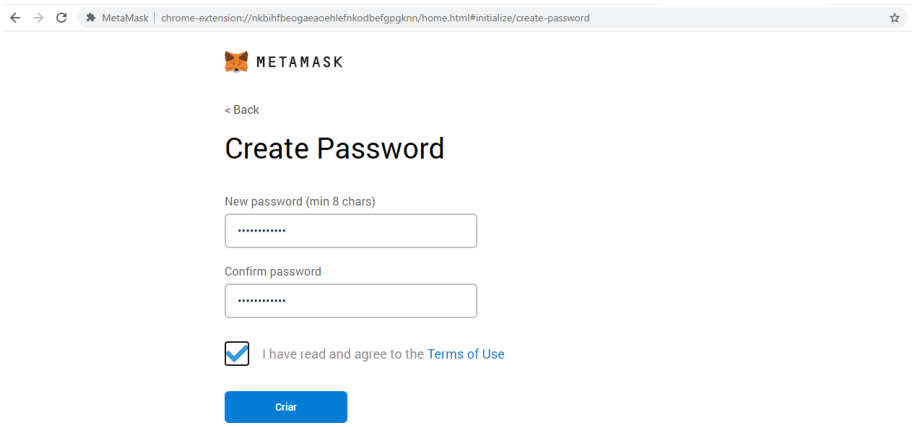


Figura 45 – Informar senha e aceitar os termos do MetaMask.

Existe um momento importante para anotar as palavras chaves para utilizar na etapa seguinte da instalação ou no caso da recuperação da conta caso necessário. Para isso, basta clicar no cadeado para visualizar as palavras chaves e depois clicar em seguinte para continuar a instalação (Figuras 46 e 47).

Depois é necessário confirmar as palavras chaves apresentadas na etapa anterior.

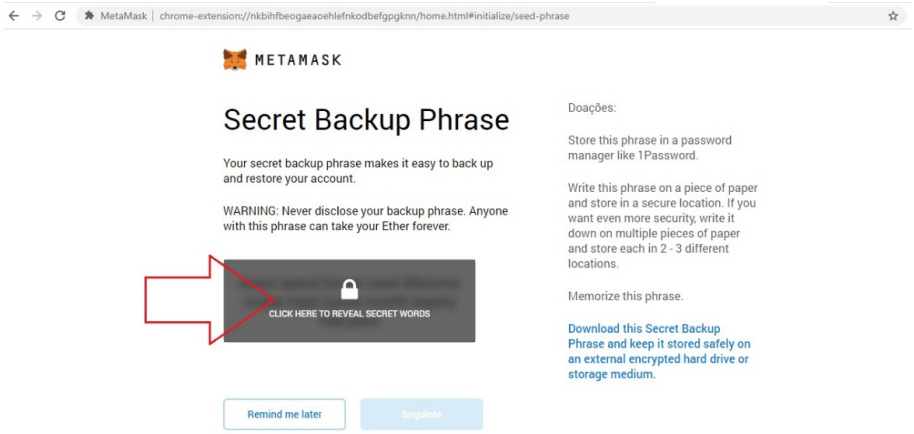


Figura 46 – Acesso as palavras chaves da conta MetaMask.

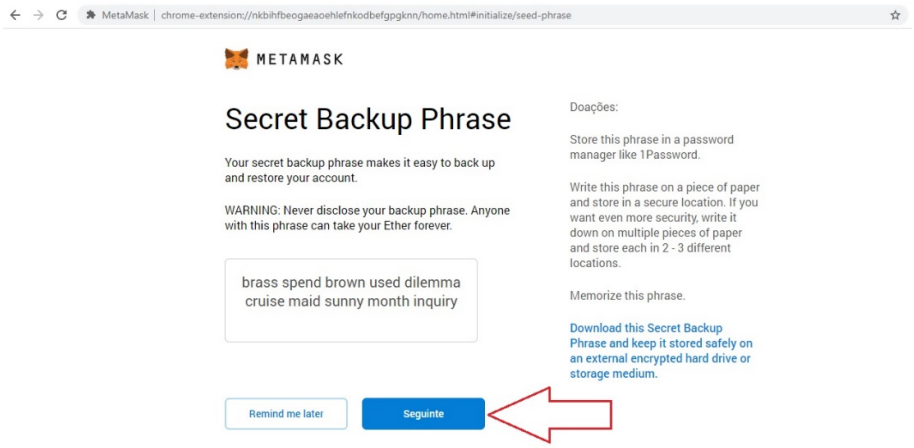


Figura 47 – Visualizar as palavras chaves da conta MetaMask.

Para isso, basta ir selecionando as palavras na mesma ordem que apareceram na etapa anterior e depois clicar em confirmar (Figura 48).

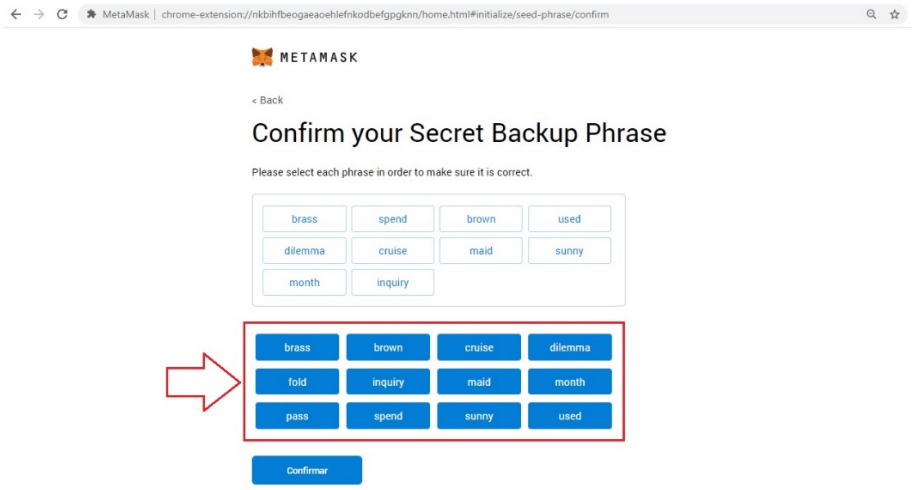


Figura 48 – Confirmar as palavras chaves da conta MetaMask.

A Figura 49 representa a confirmação que a conta foi criada com sucesso e para

iniciar o uso do MetaMask clica-se em “All Done”. A tela inicial do MetaMask pode ser visualizada na Figura 50.

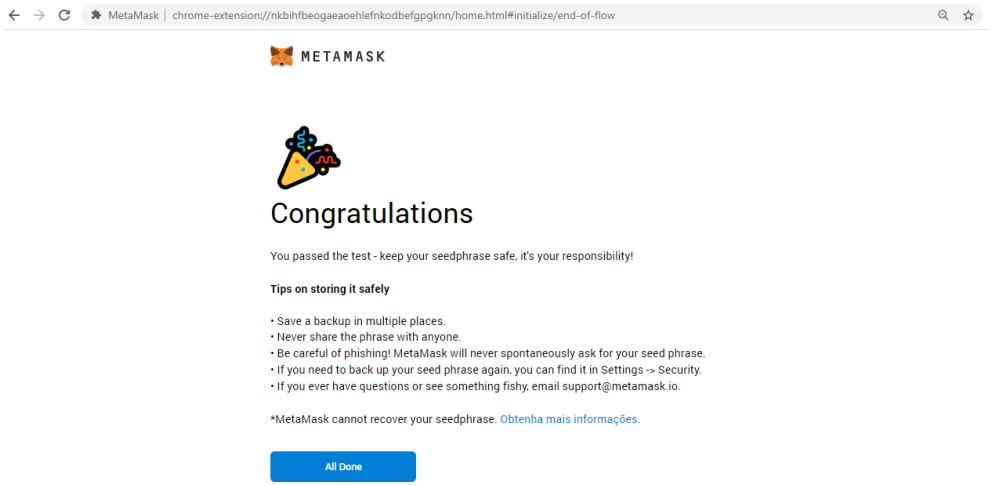


Figura 49 – Confirmação que a conta foi criada com sucesso.

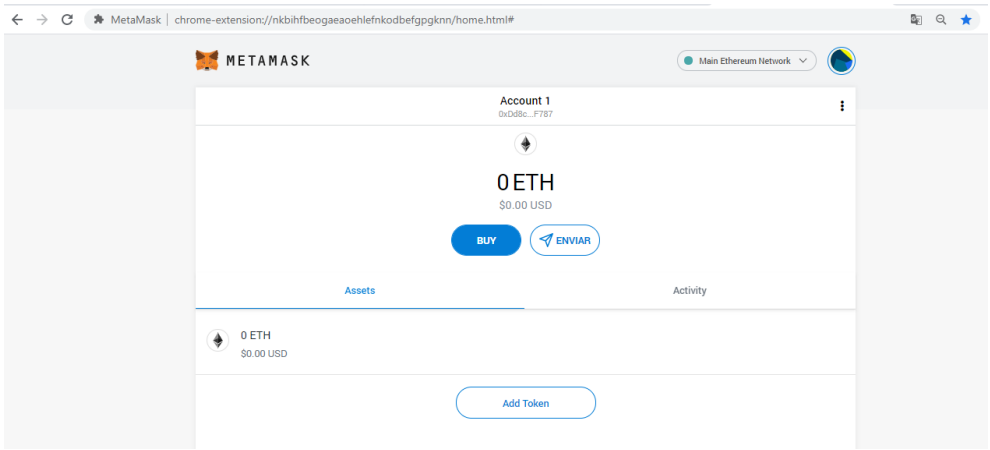


Figura 50 – Tela inicial do MetaMask.

A.2 Conseguir Criptomoeda para Testes

Para executar as funções da aplicação Educ-Dapp é necessário ter *criptomoeda* na carteira MetaMask. Por questões financeiras, iremos utilizar uma rede de testes da Ethereum para avaliar a aplicação, em que a mesma utilizar *criptomoeda* falsa. Assim não teremos gastos financeiros reais para avaliação da aplicação. Para conseguir *criptomoeda* falsa basta seguir os passos a seguir.

Na tela inicial do MetaMask selecione a rede de testes chamada Ropsten (Figura 51), em que será o ambiente selecionado para realizar todos os testes da aplicação Educ-Dapp.

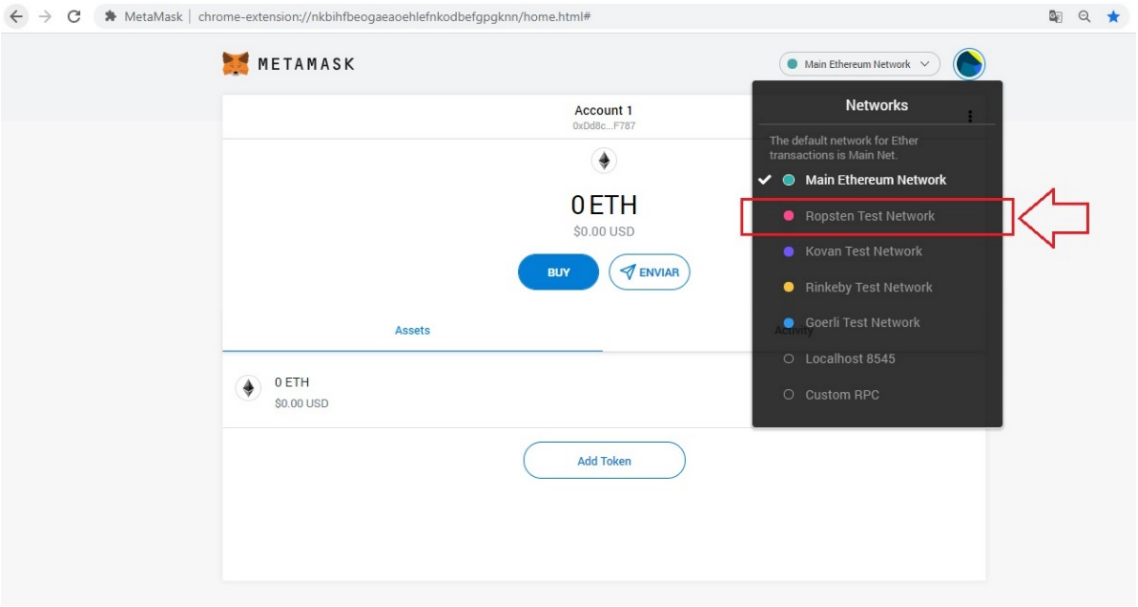


Figura 51 – Selecionar rede de testes da Ethereum.

Existem alguns sites em que é possível conseguir Ether (criptomoeda da Ethereum) falso. Abaixo será apresentado duas opções, em que só basta requisitar 1 Ether, pois essa quantidade foi observada como suficiente para realizar todos os testes da aplicação. Porém, caso precisar de mais, basta realizar novas solicitações para conseguir mais Ether.

Opção 1 - acesse o link: <https://faucet.metamask.io/>.

A Figura 52 apresenta o botão onde clicar para solicitar 1 Ether falso. Vai abrir uma tela do MetaMask pedindo autorização para o site se conectar ao mesmo e transferir o Ether solicitado, então basta aceitar e prosseguir (Figuras 53 e 54). Caso a operação for bem-sucedida vai aparecer o *hash* da transação realizada do site para conta do MetaMask utilizada no navegador (Figura 55).

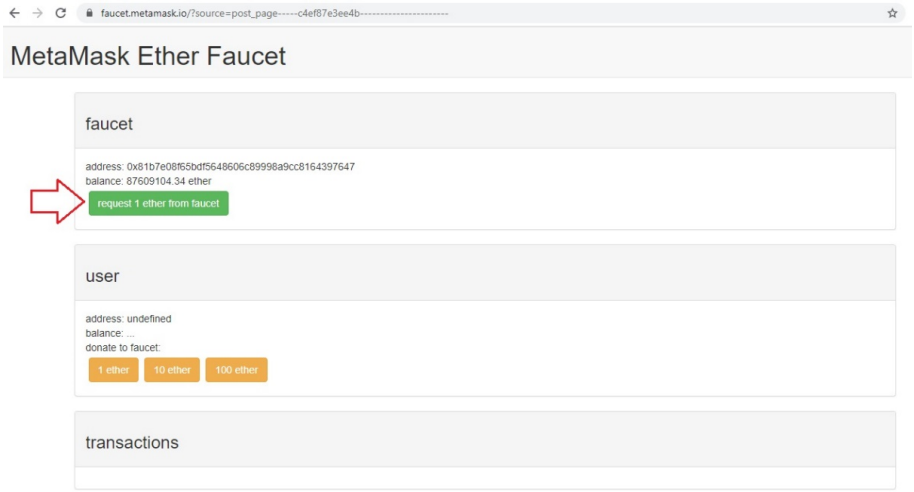


Figura 52 – Requisitar 1 Ether falso.

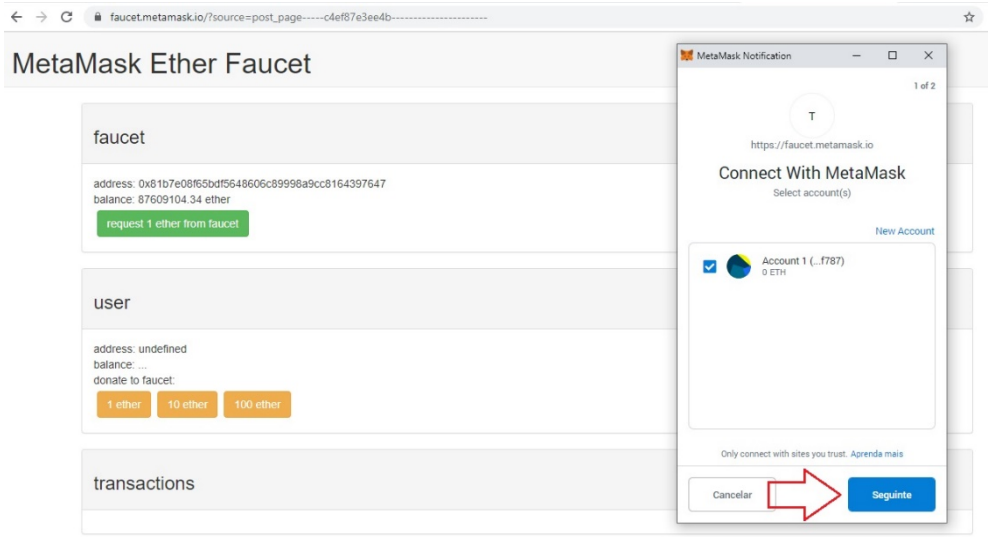


Figura 53 – Seguir para confirmação da transferência de 1 Ether.

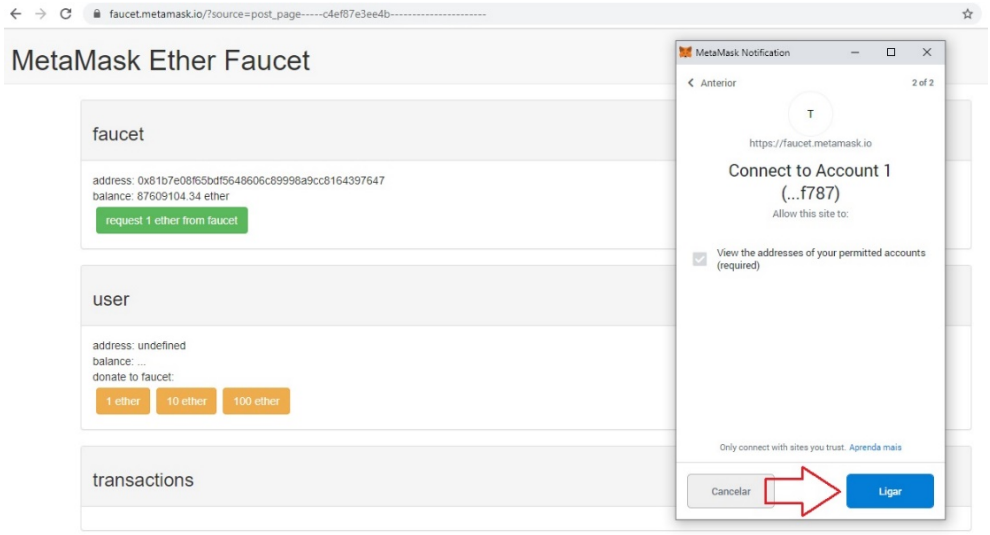


Figura 54 – Confirmação para transferência de 1 Ether.

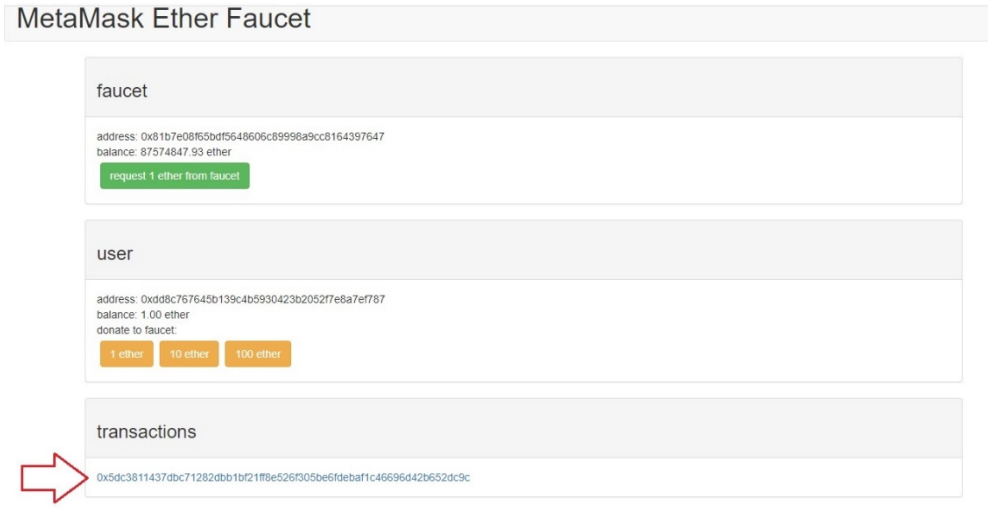


Figura 55 – *Hash* da transferência de 1 Ether do site opção 1

Opção 2 - acesse o link: <https://faucet.ropsten.be/>.

Para utilizar essa segunda opção é necessário ir primeiro na tela inicial do MetaMask e copiar o endereço da carteira de *criptomoeda* clicando em cima dos dados da conta (Figura 56). Depois acessa o site da opção 2 e basta colar o endereço da conta do MetaMask no campo informado e clicar em solicitar (Figura 57).

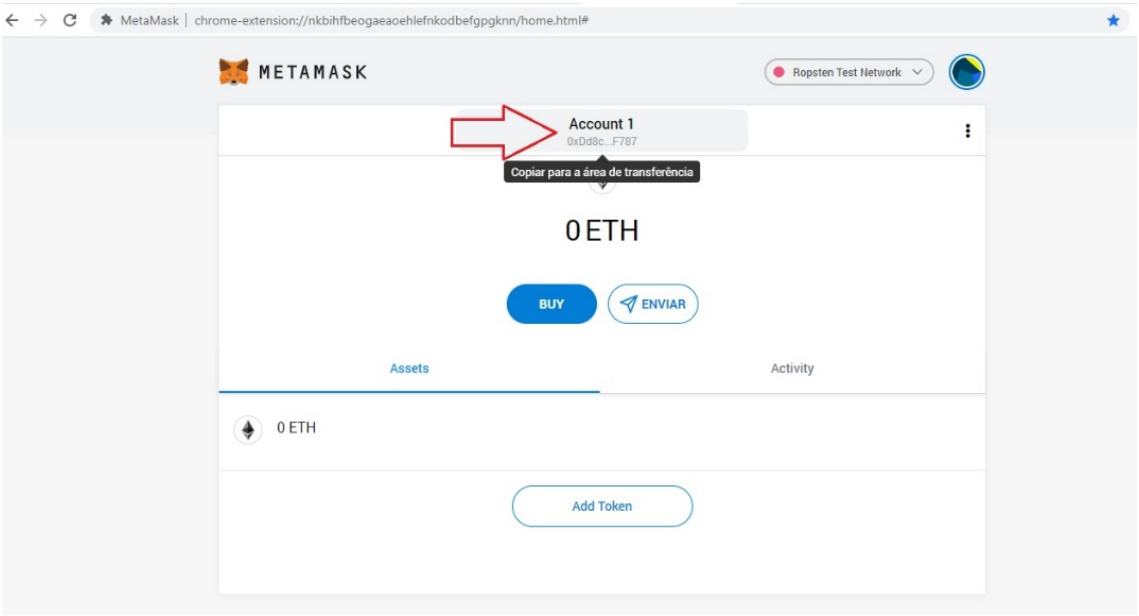


Figura 56 – Copiar endereço da conta MetaMask.

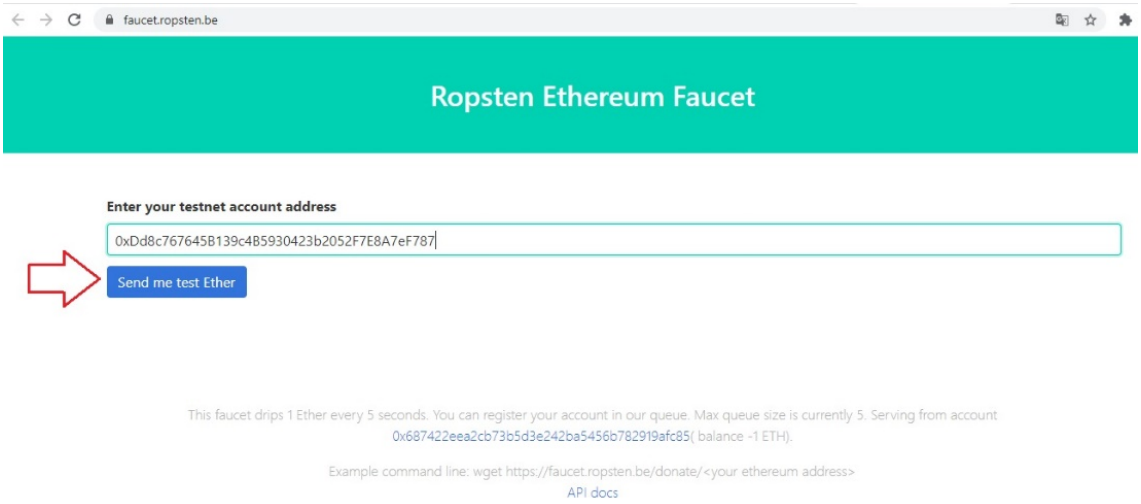


Figura 57 – Campo para informar endereço da conta MetaMask.

Caso a operação for bem-sucedida vai aparecer o *hash* da transação realizada do site para conta do MetaMask utilizada no navegador (Figura 58). Ao retornar na tela inicial do MetaMask vai visualizar 1 Ether na sua carteira, com isso, já pode utilizar as funcionalidades da

aplicação Educ-Dapp (Figura 59).

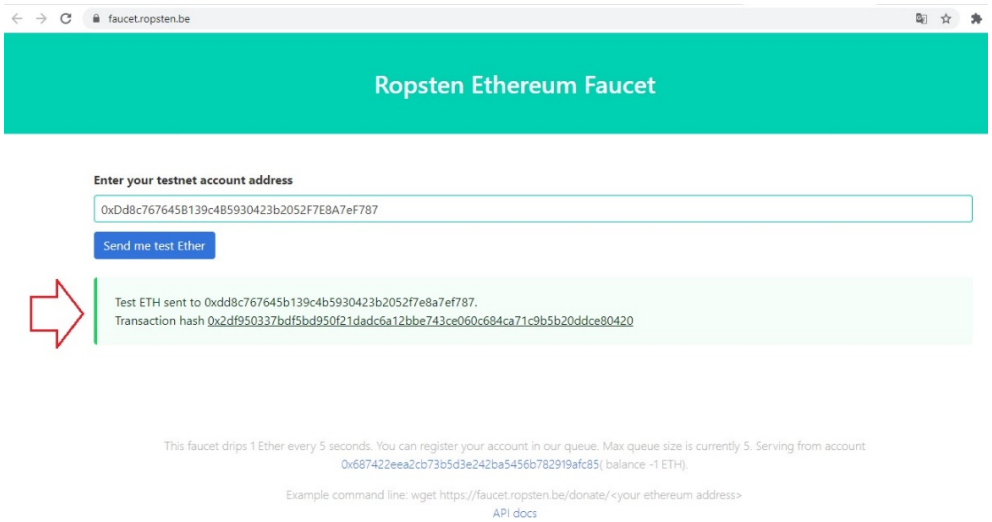


Figura 58 – *Hash* da transferência de 1 Ether do site opção 2.

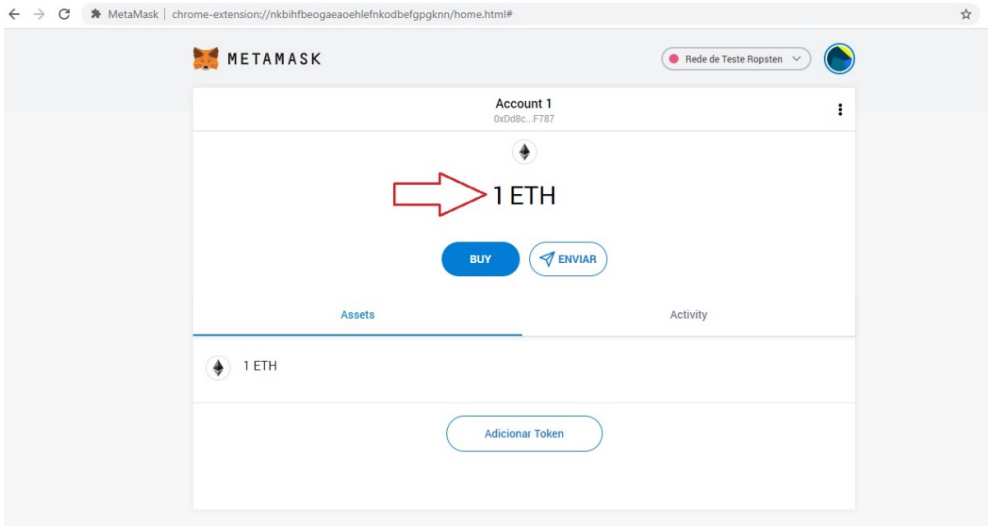


Figura 59 – Valor de 1 Ether na conta do MetaMask.

APÊNDICE B – MANUAL DE UTILIZAÇÃO DA EDUC-DAPP

Aplicação Educ-Dapp é um protótipo de uma aplicação baseada em *blockchain* que tem a função de cadastrar Instituições de Educação Superior para cadastrarem e revogarem seus diplomas emitidos. Para executar essas funções é necessário ter instalado a extensão MetaMask no seu navegador e também tem que fazer login no mesmo antes de acessar a aplicação. Existe também uma consulta pública para qualquer entidade verificar os diplomas cadastrados.

Uma observação importante é que os dados utilizados na aplicação devem ser fictícios, pois se trata de um protótipo para simulação. Porém, apesar dos dados serem fictícios, os mesmos devem ter uma estrutura e formatação que façam sentido o uso na aplicação. Os dados serão utilizados apenas para fins acadêmicos e científicos.

Foi criado um domínio temporário somente para avaliar a aplicação, em que pode ser acessada através dessa URL: <http://ufcpcompquixada.epizy.com/index.html>. Página inicial com algumas informações sobre a aplicação:

Figura 60 – Página principal da aplicação Educ-Dapp.

Será utilizada uma rede de testes da plataforma Ethereum para realizar a validação. Porém, para termos uma visão mais próxima do ambiente real da Ethereum, é interessante utilizar

a média atual de Gwei por unidade de Gas informada no site <https://etherscan.io/gastracker>, assim os valores em Ether gastos nas transações serão gerados de acordo com situação atual do mercado de *criptomoeda* da Ethereum. No momento que este documento foi criado a média estava 65 Gwei (Figura 61). Esse valor basta informar no MetaMask no momento de executar as transações.

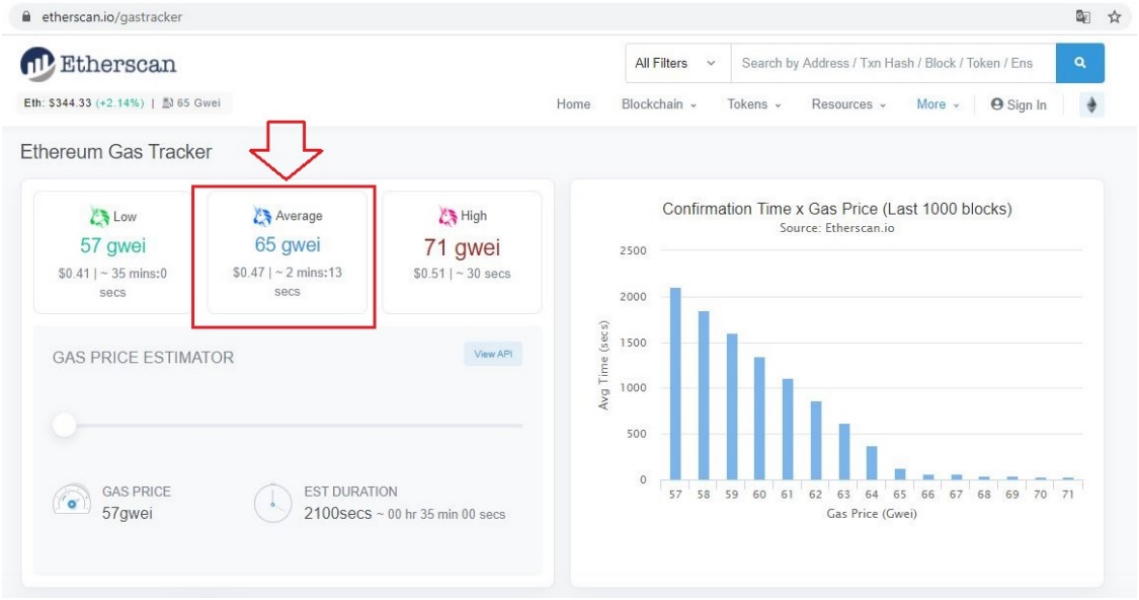


Figura 61 – Média de Gwei.

B.1 Cadastrar IES

Como forma de propor um processo global que envolva as principais entidades ligadas ao processo de emissão e registros de certificados das IES, foi criado um perfil para simular a entidade “governo” e outro para simular a entidade “IES” na aplicação. O governo tem a função de cadastrar as IES que são reconhecidas, ou seja, quem podem cadastrar diplomas na aplicação. Essa é uma forma de controle para simular a interação de órgãos públicos (por exemplo, o MEC) com aplicação. Inicialmente é necessário acessar a área de login da aplicação, isso pode ser observado na Figura 62.

Ao acessar a área de login o MetaMask vai solicitar para se conectar com aplicação, então basta aceitar (Figuras 63 e 64). Em seguida basta acessar a tela de login como mostra a Figura 65.

O próximo passo é fazer login com o perfil do governo. Utilize os seguintes dados para realizar login com o perfil do governo: usuário GovernoBrasil-MEC e senha 546529. Esse

Figura 62 – Acessar área de login da aplicação.

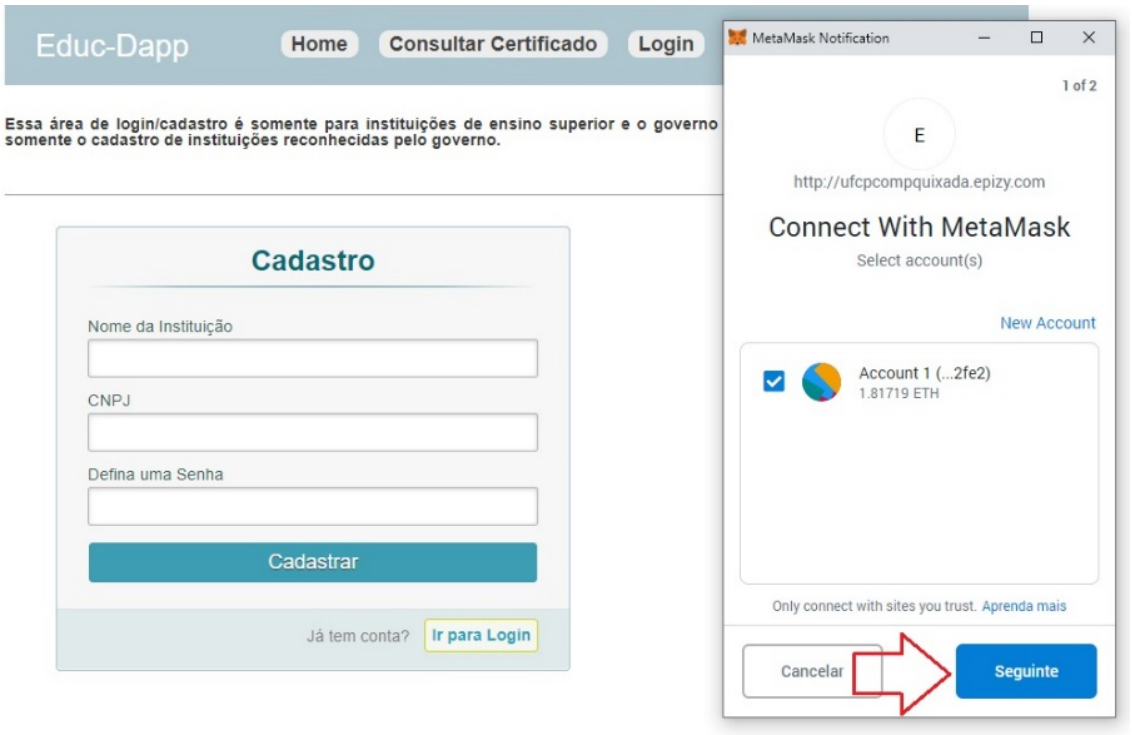


Figura 63 – Seguir para confirmação do MetaMask para interagir com aplicação.

perfil foi criado previamente como padrão para simular o acesso do governo. A Figura 66 mostra o momento do login.

A próxima etapa é cadastrar a instituição para ser reconhecida, ou seja, ter a permissão para cadastrar e revogar diplomas na aplicação. Por se tratar de uma simulação, o cadastro é simples, em que basta informar o nome e CNPJ da instituição (Figura 67).

No cadastro da IES pelo governo o MetaMask informa o valor em Ether que será

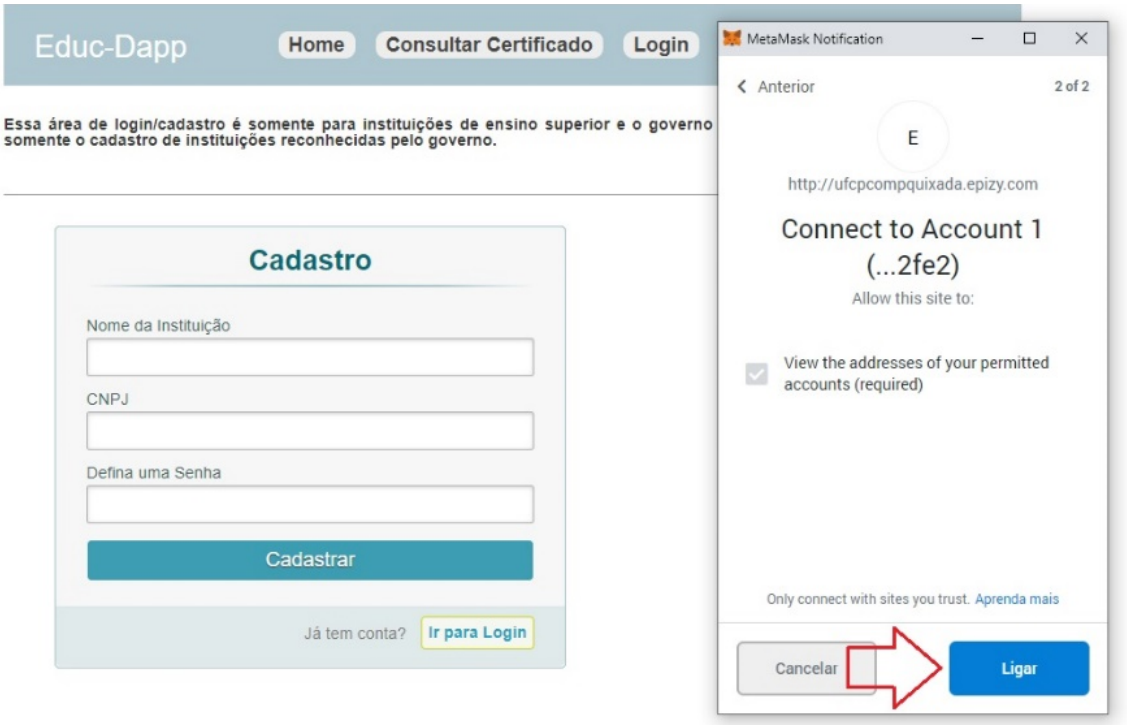


Figura 64 – Confirmação do MetaMask para interagir com aplicação.

Figura 65 – Acessar tela de login da aplicação.

gasto nessa transação, em que nesse momento é interessante usar a média atual de Gwei por unidade de Gas informada no site <https://etherscan.io/gastracker> que monitora o mercado atual de valor da *criptomoeda* Ether. Então basta informar o valor de Gwei e confirmar para executar a transação (Figura 68).

Figura 66 – Login do governo na aplicação.

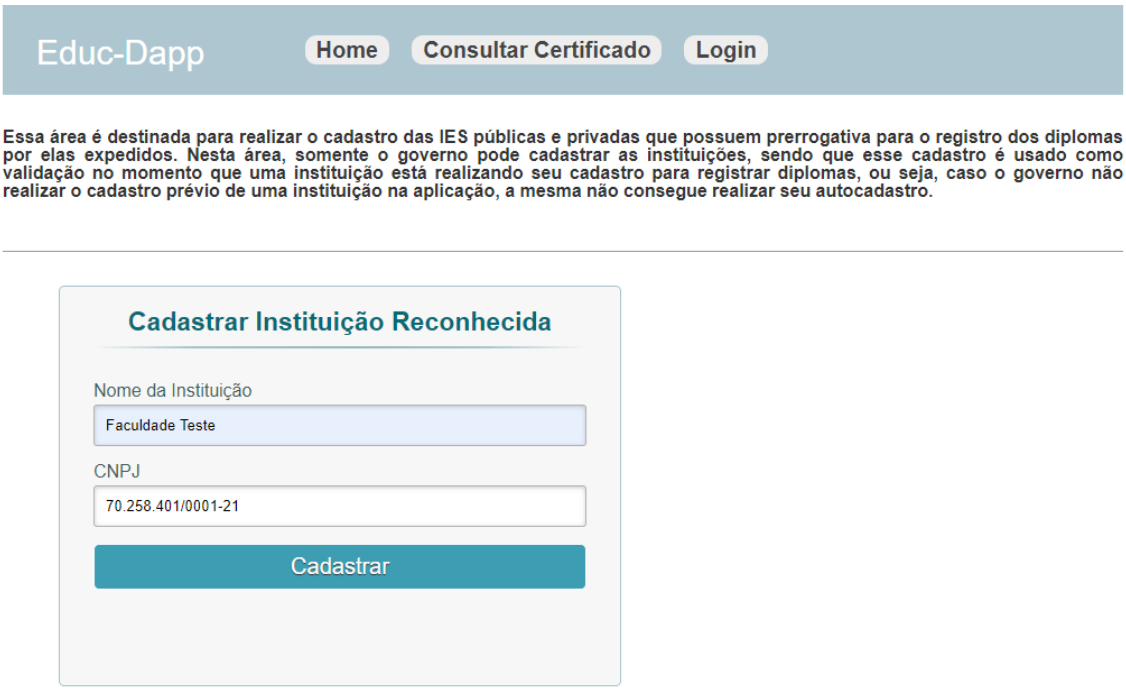


Figura 67 – Página da aplicação para cadastrar IES regular.

Com isso, a IES está habilitada a fazer o autocadastro. Para isso, basta voltar na área de login e informar os dados da IES cadastrada pelo perfil do governo e em seguida definir uma senha de acesso, depois basta clicar em cadastrar (Figura 69). Nesse momento o MetaMask informa o valor em Ether que será gasto nessa transação, em que nesse momento é interessante usar a média atual de Gwei por unidade de Gas informada no site <https://etherscan.io/gastracker>

Figura 68 – Cadastro de IES regular com confirmação do MetaMask.

para ter um valor próximo do real. Então basta informar o valor de Gwei e confirmar para executar a transação (70).

Figura 69 – Página de autocadastro da IES.

Após o autocadastro da IES é possível realizar login com os dados e ter acesso as funções cadastrar e revogar diploma. Então basta informa o usuário (CNPJ cadastrado) e senha,

Figura 70 – Autocadastro da IES com confirmação do MetaMask.

depois clicar em logar (Figura 71).

Figura 71 – Login da IES na aplicação.

B.2 Cadastrar Diploma

Para cadastrar diplomas é necessário estar logado com o perfil da IES. Após login, selecione a opção cadastrar diploma (Figura 72).

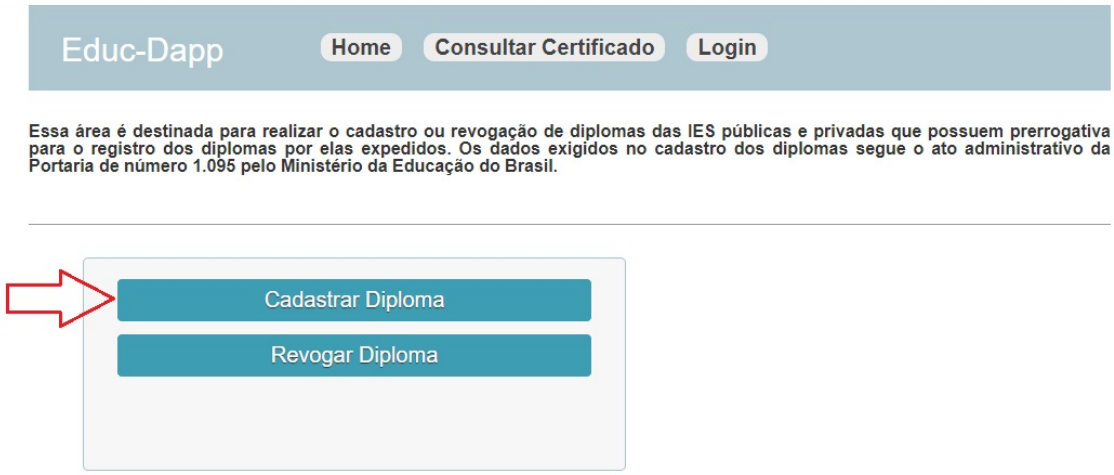


Figura 72 – Seleção de função cadastrar diplomas.

Na tela de cadastro de diploma alguns campos relacionados ao diploma serão apresentados para preenchimento. A pessoa deve preencher os campos com as informações e em seguida clicar em "Adicionar ao Lote". Pode-se adicionar ao lote quantos diplomas achar necessário e quando terminar, basta clicar em "Cadastrar". Dessa forma a aplicação vai executar uma operação de cadastrar um lote de diplomas, simulando uma colação de grau que geralmente ocorre no fim do semestre em uma IES e que envolve a emissão e registros de diplomas de vários alunos (Figura 73). Após clicar em "Cadastrar" o MetaMask informa o valor em Ether que será gasto nessa transação, em que nesse momento é interessante usar a média atual de Gwei por unidade de Gas informada no site <https://etherscan.io/gastracker> que monitora o mercado da *criptomoeda* Ether. Então basta informar o valor de Gwei e confirmar para executar a transação (74).

B.3 Consultar Diploma

Para consultar os diplomas cadastrados na aplicação basta ir em consultar certificado (Figura 75).

No momento da consulta basta informar o CPF do estudante e clicar em consultar. Em seguida a aplicação valida se existe na *blockchain* um diploma com o CPF informado. Caso

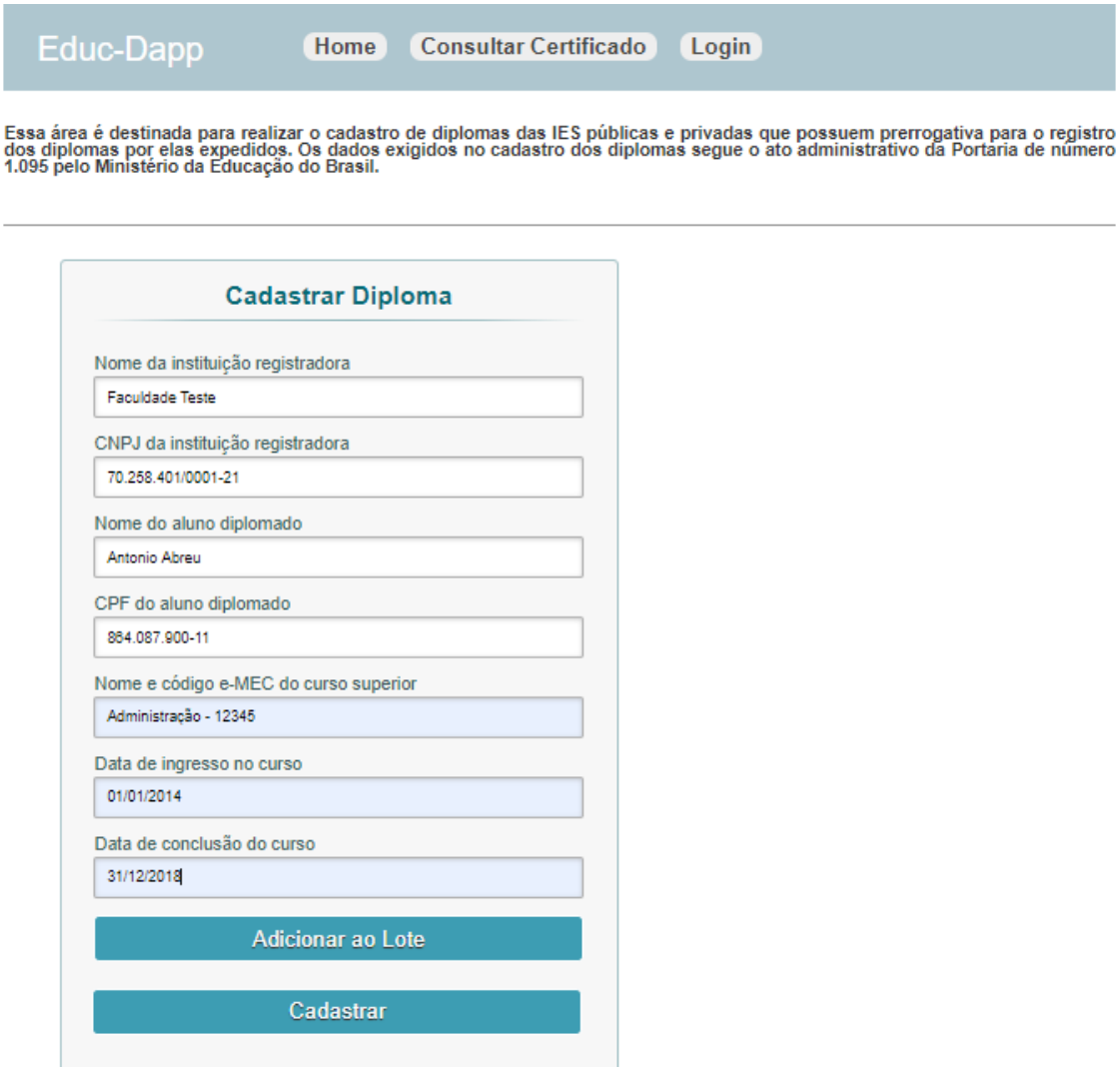


Figura 73 – Cadastro de diploma.

positivo, são apresentadas as informações do diploma. Em caso negativo, será apresentado uma mensagem informando que não existe diploma cadastrado com o CPF informado (Figuras 76 e 77).

B.4 Revogar Diploma

Revogar um diploma significa cancelar o acesso do mesmo na *blockchain*, por motivos de erros ou fraude nos dados no momento do cadastro. Para revogar é necessário estar logado com o perfil da IES. Após login, selecione a opção revogar diploma (Figura 78). Depois basta informar o CPF do aluno que deseja revogar o diploma, em seguida clicar em revogar (Figura 79).

Após clicar em revogar o MetaMask informa o valor em Ether que será gasto nessa transação, em que nesse momento é interessante usar a média atual de Gwei por unidade de Gas

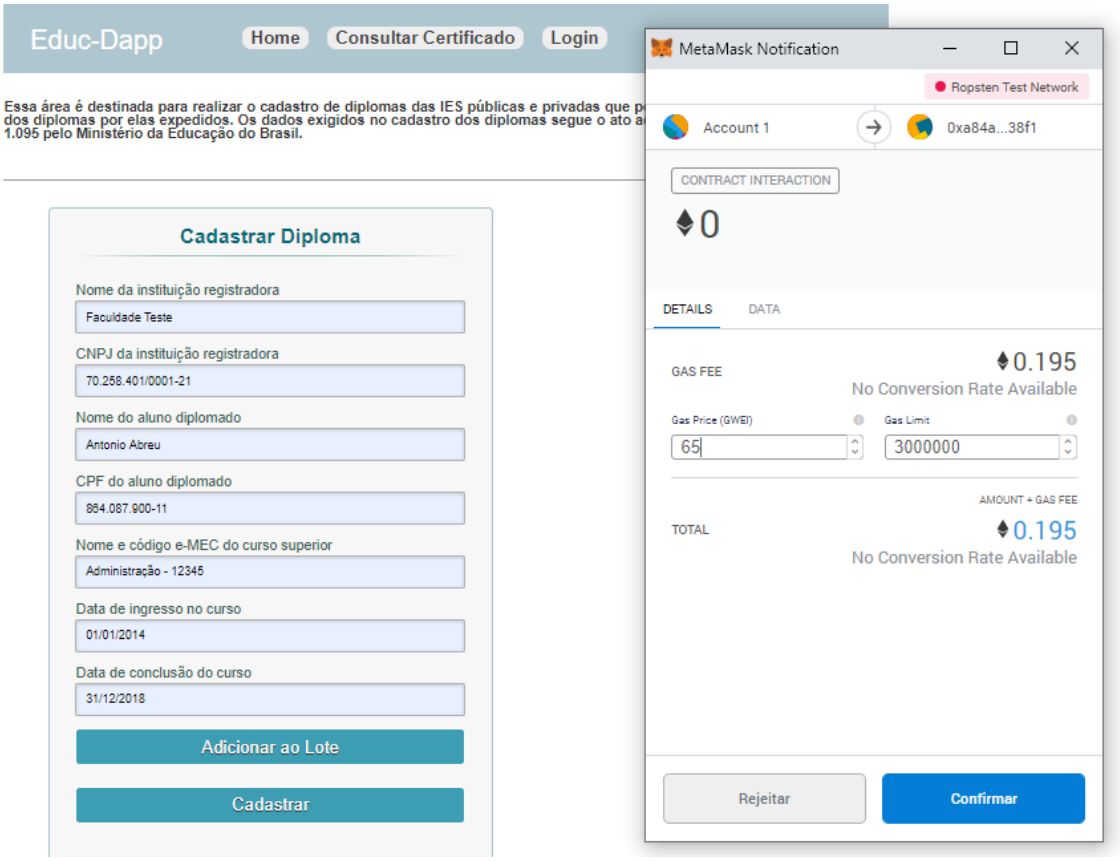


Figura 74 – Cadastro de diploma realizado pela IES.

Figura 75 – Acesso a consulta de diplomas.

informada no site <https://etherscan.io/gastracker> que monitora o mercado da *criptomoeda* Ether. Então basta informar o valor de Gwei e confirmar para executar a transação (Figura 80).

Em caso de consulta do diploma revogado, uma mensagem será apresentada informando que o diploma não está registrado, ou seja, ele não está mais disponível na *blockchain* (Figura 81). Caso queira cadastrar o diploma novamente, basta ir na função cadastrar diploma no perfil da IES e seguir os passos informados.

Figura 76 – Mensagem de validação com sucesso.

Figura 77 – Consulta e resultado da busca por diploma na blockchain.

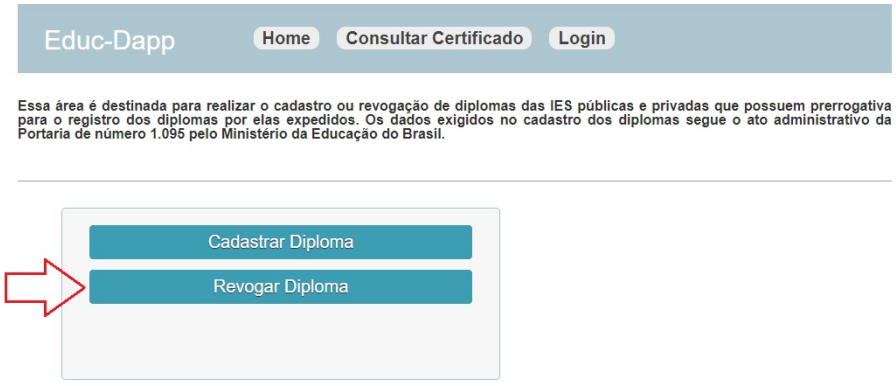


Figura 78 – Seleção de função revogar diploma

Figura 79 – Revogação de diploma.

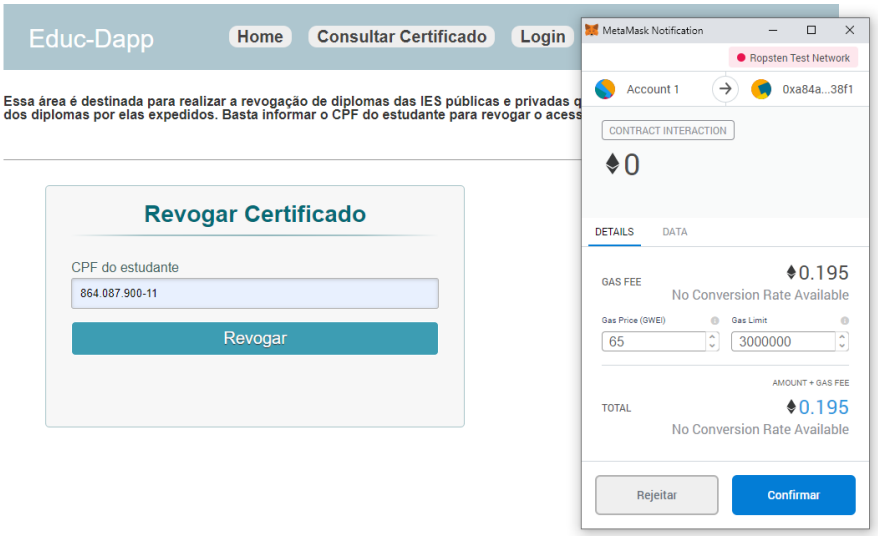


Figura 80 – Confirmação do MetaMask para Revogar de diploma.

Figura 81 – Mensagem de diploma não registrado.