Proof of Concept for Higher Education Academic Record System Using Blockchain

Bianca Figueiredo Pedrosa[1], **Reissel Reis de Souza**[1], **Diogo Silveira Mendonça**[1]

[1]Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET-RJ)
Rio de Janeiro – RJ – Brazil

{reissel.souza,bianca.pedrosa}@aluno.cefet-rj.br, diogo.mendonca@cefet-rj.br

Abstract. *The management and protection of academic data in higher education institutions is increasingly challenging due to concerns about data integrity, transparency, and availability. This paper explores the feasibility of using blockchain technology to securely store and manage academic records, such as grades, coursework, and transcripts. A prototype system was developed and evaluated for its ability to provide a secure, immutable, and transparent platform for academic data. The findings indicate that blockchain technology can effectively ensure the integrity of academic records and provide students with verified access to their information. The results suggest that blockchain has the potential to improve academic data management, providing benefits such as increased security and transparency.*

Resumo. *O gerenciamento e a proteção de dados acadêmicos em instituições de ensino superior está cada vez mais desafiador devido a preocupações sobre integridade, transparência e disponibilização de dados. Este trabalho explora a viabilidade do uso da tecnologia blockchain para armazenar e gerenciar de forma segura registros acadêmicos, como notas, curso e histórico escolar. Foi desenvolvido um sistema protótipo e avaliada a sua capacidade de fornecer uma plataforma segura, imutável e transparente para dados acadêmicos. As descobertas indicam que a tecnologia blockchain pode efetivamente garantir a integridade dos registros acadêmicos e oferecer aos alunos acesso verificado às suas informações. Os resultados sugerem que a blockchain tem o potencial de aprimorar o gerenciamento de dados acadêmicos, fornecendo benefícios como maior segurança e transparência.*

1. Introdução

A transformação digital tem impactado profundamente a gestão de informações acadêmicas. Tecnologias emergentes, como a blockchain [Nakamoto 2008], permitem o armazenamento descentralizado de dados, eliminando intermediários. No entanto, no ensino superior, ainda há uma lacuna na eficiência da gestão acadêmica, especialmente no reaproveitamento de créditos, emissão de históricos e validação de diplomas. Esses processos, gerenciados por sistemas centralizados, tendem a ser burocráticos, suscetíveis a falhas e demorados.

No estado do Rio de Janeiro ocorreu o caso do Centro Universitário da Cidade (UniverCidade) e da Universidade Gama Filho (UGF) onde essas instituições de ensino foram descredenciadas em 2014 pelo Ministério da Educação em razão da baixa qualidade

acadêmica, o grave comprometimento da situação econômico-financeira da mantenedora e a falta de um plano viável para superar o problema, além da crescente precarização da oferta da educação superior [Ministério da Educação 2014].

Por conta do descredenciamento, diversos alunos não conseguiram emitir os seus diplomas ou fazer a transferência para alguma outra instituição de ensino por não terem mais acesso aos documentos físicos que estavam em poder dos representantes legais [Bom Dia Rio 2019]. Atualmente, com a adoção das assinaturas eletrônicas, esse problema pode ser resolvido de forma totalmente digital por não mais necessitar de cópias físicas de documentos para validar o seu formato digital [Planalto 2020].

Diversas instituições de ensino superior possuem programas de ingresso para pessoas que já possuem diploma de ensino em cursos relacionados, favorecendo a aquisição de uma segunda formação acadêmica sem a necessidade de nova realização de vestibular, permitindo aproveitar o currículo acadêmico conquistado no novo curso, não precisando cursar disciplinas já vencidas em formações anteriores, em acordo com a Lei Brasileira número 9394 de 1996 [Planalto 1996].

Este trabalho propõe uma solução para otimizar a gestão de dados acadêmicos por meio da tecnologia blockchain *Ethereum* [Buterin 2014] por meio de um *smart contract* [Ramamurthy 2020] e uma aplicação frontend que interage com esse contrato por meio da MetaMask [MetaMask 2025]. A ideia central é oferecer um sistema descentralizado que permita às instituições registrarem, com segurança, disciplinas cursadas, notas e os dados dos alunos, garantindo-lhes acesso a essas informações sem a dependência da instituição. A blockchain oferece vantagens como imutabilidade, segurança criptográfica e transparência, assegurando a integridade dos dados e eliminando a necessidade de intermediários na validação.

O protótipo desenvolvido permitiu a inserção de dados de instituições de forma pública e acessível, além de garantir a segurança de dados pessoais dos alunos por meio do uso de criptografia e descriptografia na aplicação frontend usando funções do MetaMask; os alunos e a sua respectiva instituição são capazes de permitir que outras contas da rede possam acessar os seus dados.

Foi quantificado o gas das transações realizadas na blockchain da Ethereum para executar todo o fluxo de cadastro de uma instituição com um curso possuindo uma disciplina, um aluno e sua nota nessa disciplina, e chegou-se ao valor de 9.335.879 *gas*. Foi observado que o uso de outras redes *EVM-Compatible* pode reduzir significativamente a carga monetária necessária para realizar as requisições necessárias, barateando o uso da solução proposta e, consequentemente, facilitando a sua adoção por parte das instituições de ensino superior.

O restante deste trabalho está organizado como descrito a seguir. A Seção 2 explora os trabalhos com propostas semelhantes ou com contribuições aproveitadas; apresentando a solução proposta por este trabalho de forma mais profunda na Seção 3; realizando a argumentação dos resultados obtidos na Seção 4 e, por fim, com o desfecho na Seção 5 elucidando as contribuições desse trabalho.

2. Trabalhos relacionados

O estudo de Tahora et al. [Tahora et al. 2023] investiga os benefícios e desafios da implementação da blockchain na gestão do ensino superior. Os autores destacam que a blockchain reforça a privacidade e a segurança ao possibilitar o armazenamento seguro de dados por meio de criptografia, garantindo que apenas partes autorizadas tenham acesso às informações. Além disso, a tecnologia pode aprimorar a transparência por meio de registros imutáveis e contratos inteligentes, automatizando processos como emissão de históricos acadêmicos e verificação de diplomas. No entanto, sua implementação enfrenta desafios significativos, incluindo a complexidade tecnológica, que dificulta a adoção por instituições educacionais; a interoperabilidade, devido à necessidade de integração com sistemas existentes; e a escalabilidade, que impõe desafios no gerenciamento de um grande volume de usuários e transações. Os custos de implementação e manutenção da tecnologia também representam um fator crítico a ser considerado. O estudo conclui que a blockchain tem um potencial significativo para otimizar a gestão acadêmica, mas ainda há uma carência de pesquisas para viabilizar sua adoção em larga escala.

Awaji and Solaiman [Awaji and Solaiman 2022] sugerem também um sistema baseado em blockchain para armazenamento de conquistas acadêmicas no ensino superior que gera um registro confiável dessas conquistas, sanando assim o desafio crescente de verificar a autenticidade de conquistas acadêmicas como CVs e diplomas. O sistema proposto por Awaji and Solaiman [Awaji and Solaiman 2022] busca facilitar o processo de autenticação e validação de certificados de forma confiável, fácil e rápida, fazendo uso dos recursos únicos oferecidos pela tecnologia da blockchain e dos smart contracts. No trabalho desenvolvido, foi feita uma comparação com diversas outras soluções existentes para acreditação, verificação, controle de privacidade, transparência, experiência do usuário, acessibilidade e compartilhamento de registros, e observou-se que a solução proposta no trabalho atendia a todos os critérios em sua totalidade, enquanto algumas das alternativas os atendiam parcialmente ou até mesmo não forneciam uma solução para aquele ponto analisado.

Turkanovic et al. [Turkanović et al. 2018] propõem também, com o uso da blockchain, uma plataforma global de crédito de ensino superior, EduCTX. Essa plataforma é baseada no conceito do Sistema Europeu de Transferência e Acumulação de Crédito (European Credit Transfer and Accumulation System - ECTS), que é um instrumento utilizado no Ensino Superior Europeu que ajuda os estudantes a deslocar-se entre os países da União Europeia e a obter o reconhecimento das suas qualificações acadêmicas e dos períodos de estudo fora do seu país de origem, permitindo que os créditos adquiridos em uma instituição de ensino superior sejam contabilizados para a obtenção de uma qualificação em outra instituição acadêmica [União Européia 1988]. A solução proposta no trabalho busca facilitar o acesso às informações de crédito dos alunos, fornecendo uma plataforma que tanto os estudantes, como as instituições de ensino possam usar, mas também outros interessados, como empregadores etc., tenham acesso aos dados dos estudantes mediante a aprovação deles.

O artigo de Souza et al. [Souza et al. 2021] recomenda um sistema para geração e validação de diplomas e certificados utilizando a rede blockchain pública Ethereum. A abordagem combina contratos inteligentes e NFTs para geração de documentos acadêmicos únicos, e o protocolo InterPlanetary File System (IPFS) para armazenamento

distribuído dos arquivos.

Costa et al. [Costa et al. 2018] exploram a combinação da tecnologia blockchain com certificação, verificação e preservação digitais. Como prova de conceito, desenvolveu-se um protótipo para registro e verificação da autenticidade de documentos digitais, permitindo que instituições de ensino registrem documentos oficiais, como diplomas e certificados, na blockchain e que interessados validem a autenticidade do documento através de seu número de registro. Os documentos registrados são automaticamente inseridos em um repositório de preservação digital. O processo de emissão e registro do diploma digital só é iniciado após a emissão do diploma tradicional em papel, assegurando que todas as verificações acadêmicas tenham sido concluídas.

O sistema desenvolvido neste trabalho aproveita os benefícios da blockchain, como privacidade e segurança, ao permitir o armazenamento e compartilhamento de dados acadêmicos. Diferente de outras abordagens, não requer a criação de um novo endereço na blockchain, utilizando a conta já existente do aluno para outras finalidades. O acesso aos registros é controlado, exigindo aprovação do aluno, e a transmissão de dados entre as contas ocorre via compartilhamento da chave pública de encriptação, distinta da chave pública da blockchain. Além de oferecer um gerenciamento abrangente de registros acadêmicos, incluindo disciplinas, notas e históricos, o sistema prioriza a proteção de dados sensíveis dos alunos por meio de criptografia, permitindo assim que ele seja executado em blockchains públicas sem riscos de vazamento de dados.

3. Sistema de Registro Acadêmico

A dificuldade de acesso a registros acadêmicos pode gerar sérios transtornos para estudantes, especialmente em casos de descredenciamento de instituições de ensino. O fechamento do Centro Universitário da Cidade (UniverCidade) e da Universidade Gama Filho (UGF), no estado do Rio de Janeiro, em 2014, evidenciou a necessidade de armazenamento de dados de forma externa à instituição [Ministério da Educação 2014].

Como resultado, muitos alunos enfrentaram dificuldades para obter seus diplomas ou realizar transferências para outras instituições, pois os documentos físicos estavam sob a guarda dos representantes legais das instituições. Mesmo após cinco anos, ainda havia relatos sobre ex-alunos que não conseguiam acesso a seus registros acadêmicos, conforme noticiado pelo G1 [Bom Dia Rio 2019].

3.1. Proposta

O presente trabalho faz uso da tecnologia da blockchain em um contexto de registro acadêmico universitário, onde são armazenadas informações referentes a instituições de ensino superior, alunos, disciplinas cursadas e suas ementas, além da emissão de histórico. Sua principal dor sanada é facilitar o acesso às informações para os casos de reaproveitamento de créditos e validação de matrícula. A democratização dessas informações pode contribuir quando um aluno busca reaproveitar as disciplinas vencidas em outra instituição de ensino em um novo curso de ensino superior. Essa solução se propõe a ser um registro acadêmico, buscando fornecer o histórico escolar do aluno e não mais que isso, oferecendo somente funcionalidades para inserção e leitura de dados.

No desenvolvimento dessa solução foi utilizada a blockchain Ethereum com o objetivo de fornecer para as instituições de ensino superior um sistema que é acrescido com

dados dos discentes pela instituição. Permite também o acesso às informações por parte dos alunos e por contas por eles permitidas. Esse projeto é composto de duas partes: um smart contract[1] desenvolvido na linguagem Solidity e uma aplicação frontend protótipo, desenvolvida em Javascript[2]. A aplicação frontend utiliza bibliotecas para interagir com o contrato por meio da extensão do navegador da MetaMask, garantindo assim que todas as transações sejam realizadas por meio da extensão e solicitando sempre a aprovação do usuário para suas efetivações. Um vídeo de demonstração do sistema funcionando na perspectiva do usuário está disponível na web[3].

3.2. Modelagem do Sistema

A modelagem conceitual do sistema é representada pelo diagrama de classes ilustrado na Figura 1. Esse diagrama define as principais entidades envolvidas: "Institution", "Student", "Discipline" e "Grade", assim como seus atributos e relações, servindo como base para a implementação do contrato inteligente.

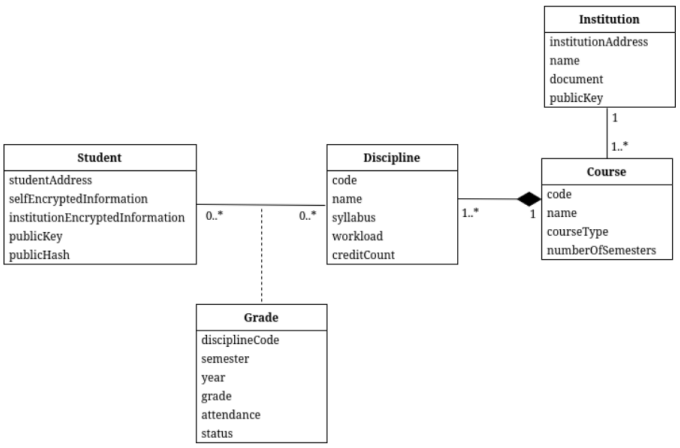

Figura 1. Diagrama de classes.

Com base nesse modelo, foram estipuladas as estruturas de dados utilizadas no smart contract para representar e gerenciar essas entidades, além das estruturas que esse contrato define para armazenar os dados necessários. As principais entidades que interagem com o contrato são: Universidade, Aluno e demais contas permitidas pelos alunos a acessarem suas informações. Outras estruturas são definidas para guardar o histórico do corpo discente durante suas atividades na instituição de ensino: Curso, Disciplina e Nota.

3.3. Segurança da informação na blockchain

Devida à natureza pública da tecnologia da blockchain, toda e qualquer informação pessoal não pode ser armazenada de forma bruta e sem consentimento, pois isso fere a Lei Geral de Proteção de Dados (LGPD), Lei Brasileira número 13.709 de 14 de agosto de 2018 [Planalto 2018], e também apresenta um risco para o dono da conta cujo endereço está associado ao dado pessoal na rede.

[1]Código fonte disponível em: https://github.com/Reissel/academic-record-blockchain
[2]Código fonte disponível em: https://github.com/bifipe/academic-registry-web
[3]Vídeo demonstração disponível em: https://youtu.be/cixm6MI6TGo

Para garantir que os dados estivessem seguros na blockchain foi utilizada uma combinação de funções existentes da MetaMask que permitem a criptografia de uma mensagem fazendo uso de uma chave de encriptação pública que é calculada a partir da chave privada da conta, solicitando a aprovação do usuário para o seu uso. A função eth_getEncryptionPublicKey retorna a chave de encriptação pública calculada a partir da conta do usuário usando a implementação Networking and Cryptography library (NaCl) do algoritmo X25519_XSalsa20_Poly1305 [4], utilizando-a para criptografar os dados antes de salvar na blockchain. Já a função eth_decrypt [5] é utilizada para descriptografar os dados a partir da mensagem criptografada ao usar a conta que originou a chave pública de encriptação. Dessa forma, ao compartilhar os dados sensíveis pela blockchain, é garantido que somente a conta que gerou a chave usada para criptografar o dado pode ter acesso a esse dado, impedindo que outras contas consigam realizar a leitura dos dados publicamente compartilhados na rede.

Visando garantir a integridade dos dados compartilhados na rede da blockchain, também é registrado para o aluno um hash gerado a partir dos seus dados pessoais. É utilizado o algoritmo SHA256 na geração do hash em conjunto com um valor aleatório de bytes que serve como salt. O salt também é registrado na blockchain de forma criptografada e, de posse desses dados, qualquer conta pode recalcular o hash salvo na rede e verificar se os valores são iguais; caso sejam diferentes, pode-se concluir que ocorreu alguma alteração nos dados e estes não são confiáveis.

3.4. Funcionalidades

Esta seção apresenta as funcionalidades do sistema, conforme requisitos apresentados na Tabela 1.

3.4.1. Cadastro de Instituição

O começo do uso do sistema é feito a partir da criação de uma instituição por parte do dono do contrato. Essa é a única interação que o dono do contrato pode realizar e somente ele pode realizar essa interação. Para acrescentar uma instituição, o dono do contrato deve informar qual é o endereço da conta da nova instituição que está sendo cadastrada, além do seu nome e um documento (alfanumérico) que permita identificar essa instituição fora da plataforma na blockchain. A partir da inserção da instituição, a conta dona do endereço cadastrado estará apta a interagir com o contrato.

3.4.2. Compartilhamento de Chave Pública de Encriptação da Instituição

O primeiro passo que a instituição deve realizar para começar o uso do sistema é compartilhar com o contrato a sua chave pública de encriptação proveniente da MetaMask; isso permitirá que os alunos usem essa chave pública para criptografar os seus dados pessoais e enviar para a Instituição para validação. Esse passo solicita aprovação da instituição

[4]Disponível em https://docs.metamask.io/wallet/reference/json-rpc-methods/eth_getencryptionpublickey. Acesso em: 02 fev. 2025

[5]Disponível em https://docs.metamask.io/wallet/reference/json-rpc-methods/eth_decrypt. Acesso em: 02 fev. 2025

para o compartilhamento da chave pública de encriptação e na confirmação da transação que salva esse dado na blockchain.

Tabela 1. Requisitos funcionais do sistema

Identificador	Requisito	Ator
RF01	Cadastrar instituição	Dono do contrato
RF02	Compartilhar chave pública de encriptação	Instituição
RF03	Cadastrar curso	Instituição
RF04	Cadastrar disciplina	Instituição
RF05	Cadastrar aluno	Instituição
RF06	Cadastrar nota do aluno	Instituição
RF07	Cadastrar informações pessoais do aluno	Aluno
RF08	Confirmar informações pessoais do aluno	Instituição
RF09	Solicitar acesso aos dados do aluno	Solicitante
RF10	Conceder permissão de acesso às informações pessoais e ao histórico do aluno	Aluno
RF11	Visualizar histórico do aluno	Instituição Aluno Solicitante com permissão

3.4.3. Cadastro de Curso e Disciplina

A inserção de cursos e suas respectivas disciplinas é feita pela instituição para possibilitar o registro das notas dos alunos e suas relações com essas estruturas. No registro de um curso, deve ser informado o código utilizado pela instituição para sua identificação, o nome do curso, o seu tipo (Bacharelado, Mestrado, etc.) e o número de semestres que o curso possui (formato numérico). Na estrutura da disciplina, é preciso informar o seu código de identificação, seu nome, a sua ementa, a carga horária e o número de créditos correspondente (esses dois últimos atributos devem ter o formato numérico).

3.4.4. Cadastro de Aluno

O cadastro de um novo aluno é feito em duas etapas, a primeira parte do registro é feita pela instituição que cadastra o aluno informando o endereço da sua conta na blockchain, atrelando o endereço da conta do aluno ao endereço da conta da instituição. A segunda parte do registro do aluno é o registro de suas informações pessoais para sua identificação.

3.4.5. Cadastro de Informações Pessoais do Aluno

De forma a garantir que o endereço na blockchain pertence a um respectivo aluno, faz-se necessário que o dono da carteira daquele endereço forneça algum documento que o

identifique fora do sistema na blockchain. Para esse projeto, é esperado o uso do Registro Geral (RG) ou do Cadastro de Pessoa Física (CPF). Por se tratar de uma informação sensível, esses dados são inseridos na blockchain de forma criptografada por meio do uso da chave pública de criptografia da instituição, de forma a só ser possível ser descriptografada pela conta da instituição que cadastrou o aluno. Também é feita uma requisição ao usuário, por meio da MetaMask, solicitando a sua aprovação para compartilhar a sua chave pública de criptografia. Além dos dados pessoais, também é gerada uma lista de bytes aleatórios (salt) que é usada no cálculo de um hash dos dados do aluno para garantir a veracidade dos dados compartilhados com os demais usuários, pois todos poderão realizar o cálculo do hash e verificar se está igual ao hash gerado no cadastro das informações do aluno. A Figura 2 ilustra todo esse processo.

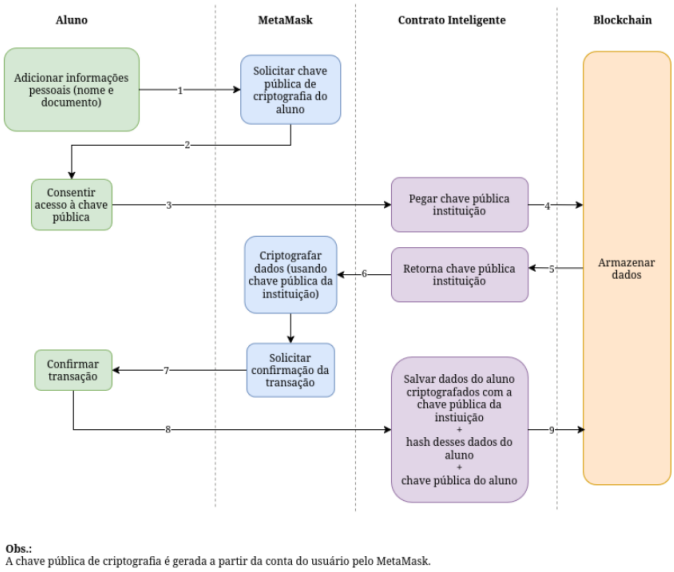

Figura 2. Criação de dados pessoais do aluno.

3.4.6. Confirmação de Informações Pessoais do Aluno

Após o aluno informar os seus dados pessoais, cabe à instituição verificar e validar a veracidade desses dados. Esse processo envolve a descriptografia dos dados pessoais do aluno, que foram criptografados com a chave da instituição e a encriptação desses dados com a chave pública que o aluno compartilhou; com isso, a instituição garante que os dados informados são verídicos e o aluno passa a poder compartilhar os seus dados com outras contas que venham a solicitar acesso a esses dados. Esse fluxo é mostrado na Figura 3.

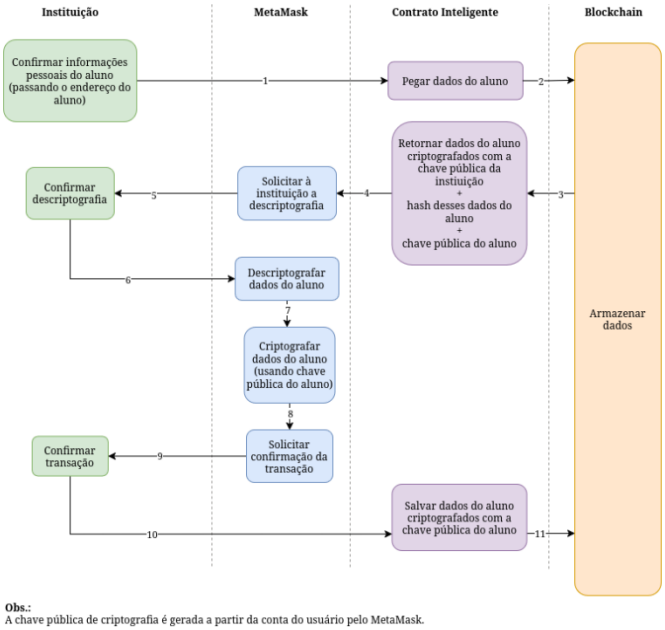

Figura 3. Confirmação das informações pessoais do aluno pela instituição.

3.4.7. Solicitação de Acesso aos Dados do Aluno

Uma conta que deseja acessar os dados pessoais e de registro acadêmico do aluno pode fazer essa requisição inserindo o endereço do aluno cujos dados deseja acessar e compartilhando também a sua chave pública de encriptação. Essa chave pública será utilizada pelo aluno para compartilhar os seus dados pessoais de forma segura com a conta solicitante, conforme demonstra a Figura 4.

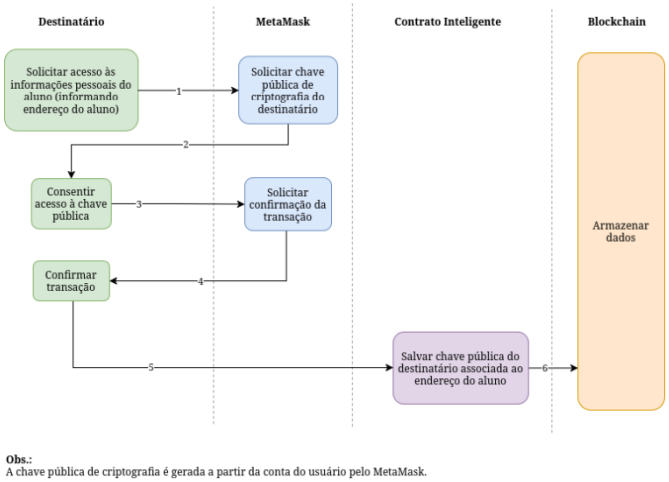

Figura 4. Solicitação de acesso aos dados pessoais do aluno.

3.4.8. Permissão de Acesso às Informações Pessoais e de Histórico Escolar do Aluno

Após uma conta solicitar ao aluno acesso aos seus dados, o aluno precisa aprovar o acesso da conta; essa aprovação é feita por meio do compartilhamento dos dados pessoais do

aluno com a conta solicitante. O aluno descriptografa os seus dados com a sua própria chave pública e salva na blockchain uma cópia encriptada com a chave pública da conta que solicitou o acesso; dessa forma, somente o dono da conta poderá pegar esses dados salvos na blockchain e descriptografar com a sua conta usando a sua chave. A Figura 5 representa essas etapas.

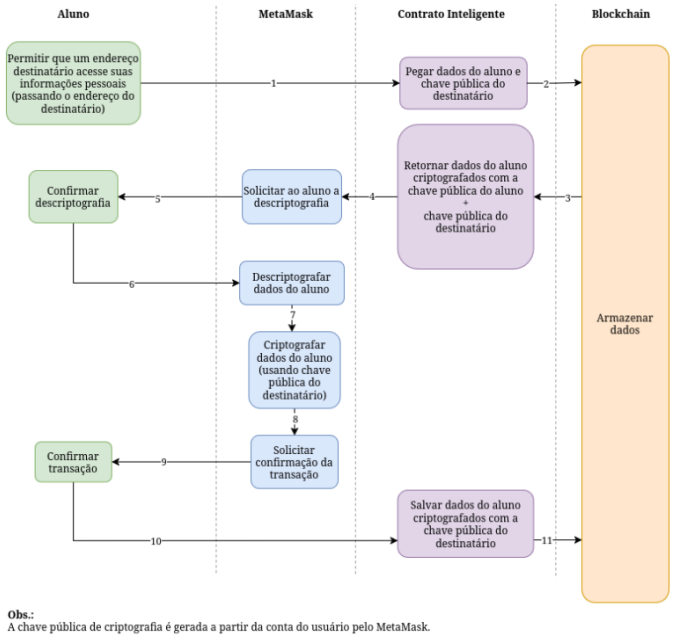

Figura 5. Permissão e acesso aos dados pessoais e ao histórico escolar do aluno.

3.4.9. Cadastro de Nota

O cadastro de nota para o aluno é feito pela instituição, para efetuar o registro das notas do aluno a instituição precisa informar o endereço da conta do aluno, código do curso, código da disciplina, semestre que se refere (1 ou 2, para 1º e 2º semestre, respectivamente), ano, nota do aluno, percentual de frequência (número inteiro) e o status (true ou false, Aprovado e Reprovado, respectivamente). Além desta funcionalidade, também é disponibilizada outra forma de inserir notas, fornecendo o endereço da conta do aluno, o código do curso e um arquivo JSON que contém uma lista de objetos estruturados com as informações de cada disciplina cursada.

3.4.10. Visualização das Informações Pessoais e do Histórico Escolar do Aluno

A visualização das informações pessoais e do histórico escolar do aluno pode ser feita pela instituição que cadastrou o aluno, pelo próprio aluno e por qualquer conta permitida pelo aluno, cada um com sua respectiva chave pública para realizar a descriptografia dos dados.

A instituição consegue visualizar, a partir do momento que o aluno insere esses dados pela primeira vez, uma vez que, antes de serem armazenados, esses dados são

criptografados usando a chave pública da instituição.

Para o aluno visualizar, é necessário que antes a instituição confirme suas informações pessoais cadastradas, para que assim essa instituição possa descriptografar os dados com sua chave e, em seguida, criptografar usando a chave pública do aluno, e desse modo, ele consiga descriptografar usando a sua própria chave.

Já para a conta permitida pelo aluno, essa conta precisa consentir o acesso à sua chave pública para que o aluno possa descriptografar seus dados e criptografar com a chave pública dessa conta, e assim, ser capaz de visualizar essas informações descriptografadas.

3.5. Qualidade do Smart Contract

De forma a aumentar a segurança na solução fornecida por este trabalho, foram utilizadas ferramentas de avaliação de vulnerabilidades disponíveis de forma gratuita e online. Essas ferramentas avaliaram a segurança do contrato por meio de parâmetros em testes estáticos que observam os riscos apresentados pelo contrato.

Em uma primeira ferramenta fornecida pela Cred Shields[6], o contrato desenvolvido recebeu a pontuação de 90.91/100 para baixo risco nas avaliações de vulnerabilidades e risco de fraudes e uma pontuação de segurança de 79.32/100, reportando 8 pontos de médio risco e 3 de baixo risco, porém nenhum ponto crítico ou de alto risco.

Uma outra ferramenta utilizada na avaliação foi a Solidity Analyzer desenvolvida pela IARD Solutions[7]. Na avaliação feita por essa ferramenta, foram relatados pontos de melhoria; entretanto, focou-se mais na qualidade do código e não em riscos encontrados no contrato. Estes pontos levantados foram corrigidos e a ferramenta não aponta mais pontos de melhoria de acordo com o algoritmo criado pela IARD Solutions.

Em adição às ferramentas anteriormente citadas, foi executada uma verificação na ferramenta de análise de segurança Mythril[8], que é capaz de detectar vulnerabilidades de segurança em smart contracts construídos para a rede Ethereum e outras redes EVM-compatíveis, que possui um algoritmo baseado em execução simbólica, e nenhum problema foi relatado. O comando invocado para realizar a análise pelo Mythril foi o *myth analyze AcademicRegistry.sol* utilizando-se assim os valores padrão de parâmetros usados pela ferramenta.

4. Discussão

Durante o uso da aplicação, foram observados alguns pontos que se reproduzem em possíveis melhorias e/ou limitações encontradas por conta do seu uso de uma rede da blockchain.

A restrição de acesso aos dados dos alunos se dá por meio da criptografia desses dados utilizando a chave de encriptação pública da conta que terá acesso; dessa forma, esses dados só conseguem ser descriptografados por essa mesma conta. Contudo, esse processo acaba inserindo novamente os mesmos dados na blockchain; só o que é alterado é com qual chave os dados foram criptografados. Além disso, essas diversas inserções na

[6]Disponível em https://solidityscan.com/quickscan

[7]Disponível em https://solidity-analyzer.iard.solutions

[8]Disponível em https://github.com/ConsenSysDiligence/mythril

blockchain são custosas e feitas somente por parte da conta do aluno; com isso, torna-se ainda mais interessante o uso de uma rede com menor custo.

Um outro ponto que deve ser observado quanto aos custos é adicionar as diversas notas dos alunos. A transação desses registros acarretará custos para a instituição e, quanto mais caros forem os custos de uma transação na rede, maior será o valor necessário para adicionar o registro acadêmico de um aluno.

Em uma avaliação utilizando a ferramenta online REMIX IDE para estipular o custo em gas das transações, foi obtido o resultado inicial de 9.335.879 gas de custo total para executar todo o fluxo; sendo isso correspondente a uma instituição com um curso e uma disciplina, um aluno cadastrado com uma nota associada ao curso e disciplina e uma conta solicitante com acesso aos dados do aluno. Com esse valor de gas, utilizando a rede Ethereum com a cotação do Ether de $2.718,76 (observada em 20/02/2025 às 20h34min), resultou em $16,75 que, convertido para real (com a cotação no mesmo dia e horário em $1 = R$5,72) equivale a R$95,84. Utilizando os mesmos valores em uma rede de segunda camada da Ethereum compatível com EVM, como a Base[9], o custo seria de $1,27 (R$7,26). A tabela 2 abaixo detalha melhor cada função e o seu custo em gas.

O processo de armazenamento dos dados usando a rede Ethereum pode ser muito custoso, por conta dos custos de transações da própria Ethereum; utilizar uma rede EVM-Compatible com custos menores de transação pode trazer um melhor custo-benefício do uso do contrato, em especial às transações que armazenam os dados pessoais do aluno criptografados, pois esses são os dados com maior tamanho armazenados na rede.

No entanto, é importante refletir sobre a viabilidade desse custo para uma implementação em larga escala, especialmente considerando a adoção por instituições públicas. A utilização de blockchains governamentais ou redes com menor custo de transação poderia tornar essa solução mais acessível e economicamente viável. Dessa forma, alternativas a redes públicas como Ethereum poderiam ser consideradas para reduzir os custos operacionais sem comprometer a segurança e a transparência do sistema.

Tabela 2. Custo de transações para as funções do contrato

Função	Gas
Deploy do contrato	3.940.132
addInstitution	239.816
addInstitutionPublicKey	103.557
addStudent	93.619
addStudentInformation	734.614
confirmStudentInformation	579.377
addCourse	163.298
addDiscipline	2.648.549
addGrade	141.656
requestAccess	111.301
addEncryptedInfoWithRecipientKey	579.960
	Total 9.335.879

[9]https://www.base.org/

5. Conclusão e Trabalhos Futuros

A principal contribuição deste estudo é a aplicação da tecnologia blockchain na gestão de registros acadêmicos, proporcionando o armazenamento seguro de históricos acadêmicos e a possibilidade de acesso controlado pelos alunos. A descentralização garante que as informações permaneçam íntegras e acessíveis, reduzindo riscos de fraudes e manipulação indevida. Além disso, a implementação de mecanismos de criptografia reforça a proteção de dados sensíveis, assegurando que apenas usuários autorizados tenham acesso a informações específicas. Apresentamos a materialização destes conceitos através de uma prova de conceito, com análise de segurança e desempenho.

No entanto, durante o desenvolvimento do processo de criptografia dos dados sensíveis dos alunos, surgiram desafios relacionados à melhor forma de garantir a segurança desses dados na blockchain. A solução adotada, baseada em métodos da MetaMask, mostrou-se uma alternativa viável no contexto atual, mas apresentou limitações, pois as funções usadas, que são dependentes da MetaMask para controle das chaves da conta, estão deprecated. Até o momento da conclusão deste trabalho, a MetaMask não disponibilizou novos algoritmos capazes de substituir esses métodos utilizados. Esse cenário pode ser diferente para outras carteiras; usando outras implementações de carteiras, pode ser possível o uso de funções que superem essa limitação apresentada pela MetaMask.

Ademais, também foi observada a necessidade de funcionalidades que permitam integrações com sistemas acadêmicos existentes nas instituições de ensino superior, buscando facilitar a inserção de dados referentes à instituição e seus cursos e disciplinas, assim como os dados dos alunos e suas notas na blockchain e, com isso, obter uma maior adesão à solução proposta.

O desenvolvimento deste sistema abre caminho para novas pesquisas na área de gestão acadêmica digital, mostrando a viabilidade do uso das novas tecnologias de blockchain, que permitem a garantia de segurança de dados, além da plena disponibilidade dos mesmos, ainda que em uma rede de acesso público. Uma possível evolução desse estudo é a integração com padrões internacionais de certificação acadêmica, o que pode ampliar sua adoção por diferentes instituições de ensino, garantindo maior interoperabilidade e reconhecimento global de diplomas e históricos acadêmicos.

Referências

Awaji, B. and Solaiman, E. (2022). Design, implementation, and evaluation of blockchain-based trusted achievement record system for students in higher education. In *Proceedings of the 5th International Conference on Information and Education Innovations*.

Bom Dia Rio (2019). Formandos da gama filho e univercidade, no rio, relatam problemas para conseguir os diplomas. Disponível em `https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/08/02/formandos-da-gama-filho-e-univercidade-no-rio-relatam-problemas-para-conseguir-os-diplomas.ghtml`. [Acessado em 31/08/2024].

Buterin, V. (2014). A next generation smart contract decentralized application platform.

Costa, R., Faustino, D., Lemos, G., Queiroga, A., Djohnnatha, C., Alves, F., Lira, J., and Pires, M. (2018). Uso não financeiro de blockchain: Um estudo de caso sobre o registro, autenticação e preservação de documentos digitais acadêmicos. In *Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações*, Porto Alegre, RS, Brasil. SBC.

MetaMask (2025). Acessado em 02/02/2025.

Ministério da Educação (2014). Mec descredencia universidade gama filho e centro universitário da cidade. Disponível em `http://portal.mec.gov.br/component/tags/tag/univercidade`. [Acessado em 31/08/2024].

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Planalto (1996). Lei nº 9.394, de 20 de dezembro de 1996. Disponível em `https://www.planalto.gov.br/ccivil_03/Leis/L9394.htm`. [Acessado em 31/08/2024].

Planalto (2018). Lei nº 13.709, de 14 de agosto de 2018. Disponível em `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm`. [Acessado em 02/02/2025].

Planalto (2020). Decreto nº 10.543, de 13 de novembro de 2020. Disponível em `http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10543.htm`. [Acessado em 01/09/2024].

Ramamurthy, B. (2020). *Blockchain in action*. Manning Publications.

Souza, E., Carneiro, E., and Coutinho, A. (2021). Geração e validação de diplomas e certificados utilizando blockchain pública. In *Anais do IV Workshop em Blockchain: Teoria, Tecnologias e Aplicações*, pages 54–59, Porto Alegre, RS, Brasil. SBC.

Tahora, S., Saha, B., Sakib, N., Shahriar, H., and Haddad, H. (2023). Blockchain technology in higher education ecosystem: unraveling the good, bad, and ugly. In *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 1047–1056. IEEE.

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., and Kamišalić, A. (2018). Eductx: A blockchain-based higher education credit platform. *IEEE Access*, 6:5112–5127.

União Européia (1988). Sistema europeu de transferência e acumulação de créditos (ects). Acessado em 18/08/2024.