COINTER PDVGT 2024
VIII Congresso Internacional de Gestão e Tecnologias

UMA APLICAÇÃO DE BLOCKCHAIN PARA ARMAZENAMENTO E VALIDAÇÃO DE CERTIFICADOS ACADÊMICOS

UMA APLICAÇÃO DE BLOCKCHAIN PARA ARMAZENAMENTO Y VALIDAÇÃO DE CERTIFICADOS ACADÊMICOS

A BLOCKCHAIN APPLICATION FOR STORAGE AND VALIDATION OF ACADEMIC CERTIFICATES

Apresentação: Comunicação Oral

Lucas Soares de Souza Cruz[1]; Prof. Me. Ronaldo Pires Borges[2]; Prof. Me. Vanessa Veloso Aragão[3]; Prof. Me. Francisco Eduardo Pires de Morais[4]

DOI: https://doi.org/10.31692/2596-0857.VIIICOINTERPDVGT.0292

RESUMO

Este trabalho apresenta os resultados do desenvolvimento de uma aplicação para o armazenamento e validação de certificados acadêmicos utilizando a tecnologia blockchain, com foco na rede Ethereum. O objetivo central foi criar um sistema seguro, descentralizado e eficiente para a emissão e gestão desses documentos, proporcionando maior autenticidade e transparência aos certificados emitidos por instituições de ensino. A fundamentação teórica baseou-se em estudos sobre a tecnologia blockchain, que oferece características de segurança, imutabilidade e descentralização, eliminando a necessidade de intermediários para a validação de informações. Além disso, foi explorado o uso de contratos inteligentes, que permitem a automação dos processos de verificação e registro de certificados. A metodologia adotada incluiu uma pesquisa-ação exploratória, apoiada por um modelo ágil de desenvolvimento baseado no Kanban, para organizar as tarefas e etapas do projeto. O processo de desenvolvimento foi dividido em ciclos iterativos, abordando a análise de requisitos, implementação e testes, com o uso de ferramentas como Solidity para a criação dos contratos inteligentes e a API RESTful para integração com o sistema. A aplicação final, CertEthereum, permite a consulta, emissão e validação de certificados acadêmicos, garantindo que esses dados sejam registrados de forma segura e imutável na blockchain Ethereum. Os resultados destacaram a eficiência do sistema CertEthereum em garantir a autenticidade e a integridade dos certificados acadêmicos. A imutabilidade dos dados, característica central da tecnologia blockchain, impede alterações posteriores, assegurando a confiabilidade dos registros. Entretanto, a pesquisa também identificou algumas limitações, como o custo variável das transações na rede Ethereum e a complexidade técnica associada à manutenção do sistema. Além disso, questões de privacidade e conformidade com a LGPD foram discutidas, indicando a necessidade de cuidados adicionais na implementação. Conclui-se que a aplicação da tecnologia blockchain na educação tem um grande potencial para transformar a gestão de documentos acadêmicos, proporcionando mais segurança e autonomia aos estudantes sobre seus registros. O trabalho sugere, como pesquisas futuras, a integração com outras plataformas educacionais, o uso de redes blockchain alternativas que apresentem menor custo e a exploração de melhorias na privacidade dos dados, para atender a requisitos legais de forma mais eficiente.

1 Tecnólogo em Análise e Desenvolvimento de Sistemas, IFPI – Campus Floriano, soareslukas9090@gmail.com
2 Professor Mestre, IFPI – Campus Floriano, ronaldo.pb@ifpi.edu.br
3 Professora Mestre, IFPI – Campus Floriano, vanessa.veloso@ifpi.edu.br
4 Professor Mestre, IFPI – Campus Floriano, professoreduardo.pires@ifpi.edu.br

Palavras-Chave: Blockchain, Certificados Acadêmicos, Ethereum, Contratos Inteligentes, Segurança de Dados.

RESUMEN
Este trabajo presenta los resultados del desarrollo de una aplicación para almacenar y validar certificados académicos utilizando tecnología blockchain, enfocado en la red Ethereum. El objetivo central fue crear un sistema seguro, descentralizado y eficiente para la emisión y gestión de estos documentos, brindando mayor autenticidad y transparencia a los certificados emitidos por las instituciones educativas. La fundamentación teórica se basó en estudios sobre la tecnología blockchain, que ofrece características de seguridad, inmutabilidad y descentralización, eliminando la necesidad de intermediarios para validar la información. Además, se exploró el uso de contratos inteligentes, que permiten automatizar los procesos de verificación y registro de certificados. La metodología adoptada incluyó investigación acción exploratoria, apoyada en un modelo de desarrollo ágil basado en Kanban, para organizar las tareas y etapas del proyecto. El proceso de desarrollo se dividió en ciclos iterativos, que abarcaron análisis de requisitos, implementación y pruebas, utilizando herramientas como Solidity para crear contratos inteligentes y la API RESTful para la integración con el sistema. La aplicación final, CertEthereum, permite la consulta, emisión y validación de certificados académicos, garantizando que estos datos queden registrados de forma segura e inmutable en la cadena de bloques Ethereum. Los resultados resaltaron la eficiencia del sistema CertEthereum para garantizar la autenticidad e integridad de los certificados académicos. La inmutabilidad de los datos, una característica central de la tecnología blockchain, evita cambios posteriores, garantizando la confiabilidad de los registros. Sin embargo, la investigación también identificó algunas limitaciones, como el costo variable de las transacciones en la red Ethereum y la complejidad técnica asociada con el mantenimiento del sistema. Además, se discutieron temas de privacidad y cumplimiento de la LGPD, indicando la necesidad de un cuidado adicional en la implementación. Se concluye que la aplicación de la tecnología blockchain en la educación tiene un gran potencial para transformar la gestión de documentos académicos, brindando más seguridad y autonomía para ellos. estudiantes sobre sus registros. El trabajo sugiere, como investigaciones futuras, la integración con otras plataformas educativas, el uso de redes blockchain alternativas que presenten menores costos y la exploración de mejoras en la privacidad de los datos, para cumplir con los requisitos legales de manera más eficiente.
Palabras Clave: Blockchain, Certificados Académicos, Ethereum, Contratos Inteligentes, Seguridad de Datos.

ABSTRACT
This paper presents the results of the development of an application for the storage and validation of academic certificates using blockchain technology, focusing on the Ethereum network. The main objective was to create a secure, decentralized and efficient system for the issuance and management of these documents, providing greater authenticity and transparency to the certificates issued by educational institutions. The theoretical basis was based on studies on blockchain technology, which offers security, immutability and decentralization characteristics, eliminating the need for intermediaries for the validation of information. In addition, the use of smart contracts was explored, which allow the automation of the processes of verification and registration of certificates. The methodology adopted included an exploratory action research, supported by an agile development model based on Kanban, to organize the tasks and stages of the project. The development process was divided into iterative cycles, addressing the analysis of requirements, implementation and testing, using tools such as Solidity for the creation of smart contracts and the RESTful API for integration with the system. The final application, CertEthereum, allows the consultation, issuance, and validation of academic certificates, ensuring that this data is recorded securely and immutably on the Ethereum blockchain. The results highlighted the efficiency of the CertEthereum system in guaranteeing the authenticity and integrity of academic certificates. The immutability of data, a central feature of blockchain technology, prevents subsequent changes, ensuring the reliability of records. However, the research also identified some limitations, such as the variable cost of transactions on the Ethereum network and the technical complexity associated with maintaining the system. In addition, privacy and compliance issues with the LGPD were discussed, indicating the need for additional care in the implementation. It is concluded that the application of blockchain technology in education has great potential to transform the management of academic

documents, providing more security and autonomy to students over their records. The work suggests, as future research, the integration with other educational platforms, the use of alternative blockchain networks that present lower costs, and the exploration of improvements in data privacy, to meet legal requirements more efficiently.
Keywords: Blockchain, Academic Certificates, Ethereum, Smart Contracts, Data Security.

INTRODUÇÃO

A tecnologia blockchain, originalmente implementada para transações de moeda virtual de forma descentralizada, com o lançamento do artigo de Nakamoto (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System", permite realizar registros e transferências sem a necessidade de uma autoridade central, utilizando provas criptográficas de trabalho e assinaturas digitais. Essa tecnologia tem sido aplicada em diversos setores, incluindo a emissão de certificados acadêmicos, reduzindo burocracias e custos administrativos. Um exemplo é o Massachusetts Institute of Technology (MIT), que em 2017 adotou a plataforma Blockcerts para emissão de diplomas em alguns cursos (M. Jirgensons; J. Kapenieks, 2018), e a Universidad Nacional de Colombia, que, em 2019, foi pioneira na América Latina ao utilizar blockchain para este fim (Agencia de Noticias U. N., 2019).

O controle de emissão de documentos em blockchain é realizado por meio de Contratos Inteligentes, programas que automatizam acordos entre partes, executando regras automaticamente quando as condições são atendidas (Ramírez, 2019). Nakamoto (2008) destaca que esses contratos são fundamentais para transações seguras e transparentes. A rede Ethereum é uma aplicação popular que utiliza blockchain e contratos inteligentes para validar informações, permitindo que terceiros acessem seus recursos computacionais com o uso do Ether, sua moeda nativa (K. Fan, 2018). Segundo Buterin (2013), os contratos inteligentes na Ethereum proporcionam um ambiente seguro e versátil para acordos automatizados, destacando-se como uma inovação essencial para a validação e armazenamento de certificados acadêmicos no cenário atual.

O uso de contratos inteligentes automatiza a verificação de certificados acadêmicos, reduzindo custos administrativos e aumentando a eficiência na emissão desses documentos, refletindo a evolução da tecnologia blockchain. Além disso, a descentralização da blockchain garante que os certificados possam ser acessados pelos alunos, mesmo que a instituição esteja indisponível ou que os dados locais sejam perdidos, assegurando acesso independente de bancos de dados específicos.

Portanto, a pesquisa teve como objetivo principal desenvolver uma aplicação *Blockchain* Ethereum por meio de contratos inteligentes para o armazenamento e validação de certificados acadêmicos. Em síntese, o objetivo é que os usuários da aplicação possam validar

a autenticidade dos certificados, economizando tempo e esforço, além disso a natureza descentralizada do blockchain permite que partes autorizadas acessem e verifiquem certificados de qualquer lugar do mundo. Ademais, esta abordagem inovadora coloca os estudantes no controle de seus próprios registros acadêmicos, permitindo que compartilhem suas credenciais de forma segura com empregadores ou outras instituições de ensino, sem a necessidade de intermediários. Este trabalho limita-se ao desenvolvimento e implantação em ambiente controlado da ferramenta CertEthereum, o software resultante da pesquisa.

FUNDAMENTAÇÃO TEÓRICA

Uma blockchain é um registro público e imutável de transações, organizado em blocos interligados e criptograficamente seguros, validando transações de forma descentralizada sem intermediários (Jain & Jain, 2019). Ela opera como um sistema de banco de dados distribuído, mantido colaborativamente em uma rede peer-to-peer (P2P), onde cada participante é responsável pela preservação e gestão dos dados (Cardoso da Cruz et al., 2018). Essa tecnologia foi desenvolvida com foco em operações seguras, armazenamento distribuído, integridade dos dados e imutabilidade das transações, oferecendo uma solução robusta para a gestão de dados em ambientes descentralizados.

Segundo Sifah et al. (2020), a blockchain é caracterizada por sua estrutura distribuída e descentralizada, onde as transações são verificadas sem uma autoridade central, utilizando provas criptográficas de trabalho, assinaturas digitais e uma rede P2P. Uma vez que um bloco é adicionado, ele se torna imutável e inviolável, e a utilização de hashes matemáticos garante a precisão e segurança dos dados armazenados. Além disso, Narayanan et al. (2016) destacam que a blockchain oferece transparência e rastreabilidade, já que todas as transações são visíveis para os participantes da rede e podem ser auditadas, resultando em um histórico confiável e verificável.

As transações em blockchain envolvem a troca de ativos digitais entre usuários, registradas de forma imutável em blocos. Cada transação é enviada a um servidor participante que a dissemina para os demais nós da rede, onde um protocolo de consenso valida e ordena as transações, criando novos blocos que garantem a segurança e transparência do sistema (Gupta & Sadogui, 2021). Segundo Ahluwalia, Mahto e Guerrero (2020), os custos de transação incluem recompensas pagas a mineradores ou validadores que processam as transações, incentivando sua participação e assegurando a integridade e funcionalidade da rede, com variações de custo conforme o congestionamento e o tipo de transação.

Existem dois principais métodos de verificação de transações em blockchain: Proof-of-

Work (PoW) e Proof-of-Stake (PoS). O PoW, utilizado originalmente pelo Bitcoin e pela Ethereum até a atualização para Ethereum 2.0, consiste em um desafio matemático complexo resolvido por mineradores, que compete pelo direito de adicionar novos blocos à rede, recebendo uma recompensa após a validação da transação (Asif & Hassan, 2023). No entanto, o PoW exige alto consumo de energia, tornando-o menos sustentável. Por isso, a Ethereum adotou o PoS, onde os validadores bloqueiam tokens, um processo chamado staking, para ganhar a chance de adicionar blocos. A seleção é baseada na quantidade de tokens apostados, proporcionando uma segurança e eficiência energética superior ao PoW (Cassez, Fuller & Asgaonkar, 2022; Lashkari & Musilek, 2021).

Zheng et al. (2020) explicam que contratos inteligentes são programas de computador que executam automaticamente cláusulas contratuais quando condições predefinidas são atendidas, eliminando a necessidade de um validador central e tornando o processamento mais rápido e seguro em uma rede blockchain peer-to-peer. Esses contratos podem ser desenvolvidos em várias plataformas, como NXT, Ethereum e Hyperledger Fabric, cada uma oferecendo ferramentas específicas, linguagens de programação especializadas e diferentes níveis de segurança para atender às necessidades do desenvolvimento de contratos inteligentes (Khan et al., 2021). No Ethereum, uma chamada de contrato é uma mensagem transmitida ao contrato na blockchain, que inicia a execução do código do contrato. Essa mensagem é empacotada como dados em uma transação e depois enviada para a rede Ethereum. A transação é registrada na blockchain, iniciando a execução do contrato (Ta; Do, 2024).

O custo de operações na rede Ethereum é definido pelo "gas", que mede o poder computacional necessário para processar ações na blockchain. O gas é calculado em Wei, a menor unidade de Ether, onde 1 Ether equivale a 10^{18} Wei; para facilitar, existe a unidade intermediária Gwei, que corresponde a 1 bilhão de Wei (Koutmos, 2023). Farokhnia e Goharshady (2023) destacam a importância da otimização do código para minimizar o consumo de gas, já que um uso excessivo pode desencorajar a criação de Dapps. Técnicas como refatoração de código, uso de ferramentas como Gasol e Gassaver, e a transferência de processamento para fora da cadeia são estratégias recomendadas para reduzir custos, embora seja essencial evitar erros que possam comprometer a eficiência da rede.

METODOLOGIA

A pesquisa adotou uma metodologia científica do tipo pesquisa-ação e exploratória. A Pesquisa-Ação, uma abordagem qualitativa que busca modificar o ambiente estudado por meio da ação do pesquisador, é utilizada para descrever tentativas de mudança em organizações ou

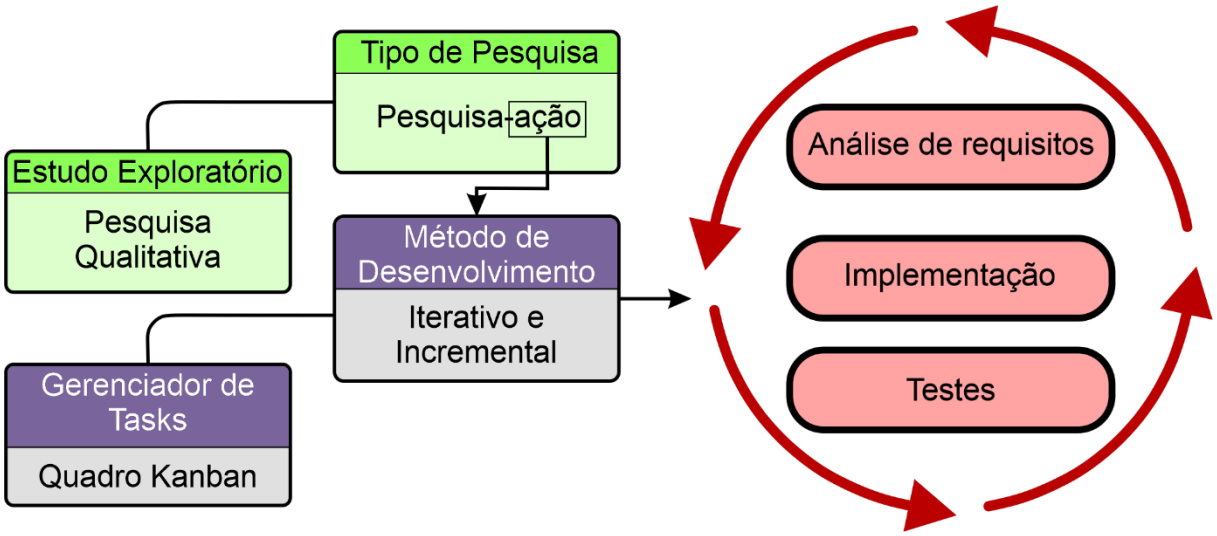
grupos através do desenvolvimento e implantação de sistemas (Wainer et al., 2007).

Para a melhor organização dos processos de criação do software e gerenciamento de tasks e etapas do desenvolvimento foi seguido o método Kanban, utilizando a ferramenta Jira. O Kanban, do japonês “Cartão”, é baseado em um quadro físico ou digital dividido em colunas que representam diferentes estágios do fluxo de trabalho. Quanto ao processo de desenvolvimento em si se seguiu o modelo iterativo e incremental, que, segundo Sommerville (2011), divide as etapas de desenvolvimento em incrementos, que incorporam uma funcionalidade ou melhoria a cada estágio, para isso, considera apenas parte dos requisitos para focar em cada ciclo.

O Kanban foi dividido em quatro partes, nomeadas: **Backlog**, responsável por conter todas as tarefas que serão executadas em algum momento do desenvolvimento. **A fazer,** que agrupa as que foram priorizadas, e estão prontas para serem iniciadas, divididas entre ‘alta prioridade’ e ‘baixa prioridade’. **Em desenvolvimento**, responsável pelas tasks que ainda estão em andamento. **Concluídas**, traz todas as tarefas que já foram finalizadas, subdivididas entre as que já foram revisadas e as que ainda estão aguardando por este processo.

A Figura 01 apresenta um resumo da metodologia deste trabalho:

Figura 01 – Etapas da metodologia



Fonte: Própria (2024).

O desenvolvimento do software seguiu três etapas principais: análise de requisitos, implementação e testes. A análise de requisitos, considerada a fase mais importante, envolveu a identificação e modelagem das necessidades do sistema, resultando na criação de um documento de Requisitos do Sistema (Selner, 1999). Essa etapa contou com entrevistas e

investigações sobre a emissão de certificados no IFPI e em cursos online. A implementação consistiu na aplicação dos requisitos utilizando as ferramentas adequadas, seguida por testes básicos do código desenvolvido. Para garantir a qualidade, foram realizados testes automatizados que verificaram a conformidade com os requisitos, uma prática essencial para o desenvolvimento seguro de software.

O fluxo da pesquisa, organizado com o Kanban, envolveu seis etapas principais: pesquisa de artigos e fontes relevantes para embasamento teórico, criação e organização do ambiente de trabalho, definição do fluxo de trabalho com quadros de tarefas ("Backlog", "A fazer", "Em desenvolvimento" e "Concluído"), limitação de tarefas para evitar sobrecarga, gerenciamento do fluxo com ajustes conforme a conclusão das tarefas e, finalmente, análise contínua para identificar melhorias e ajustes necessários no processo.

As ferramentas usadas para realização deste trabalho foram: Ethereum Blockchain, escolhida devido à sua robustez e ampla adoção para implementação de contratos inteligentes; Solidity, linguagem de programação para o desenvolvimento de contratos inteligentes na plataforma Ethereum; Alchemy SDK, ferramenta de desenvolvimento, depuração e implantação de contratos inteligentes e interações diretas com a blockchain Ethereum; Web3.py, biblioteca Python para interagir com blockchain em geral. Quando conectada à Alchemy SDK, é responsável por ser a “tradutora” de todas as operações que devem ser feitas na blockchain; Banco de Dados Relacional PostgreSQL, para armazenamento de metadados relacionados aos certificados acadêmicos e usuários do sistema. Django, framework web de alto-nível escrito em Python. É usado para construir a aplicação de forma segura, escalável e confiável; Django Rest Framework: kit de ferramentas para o framework Django para facilitar a construção de APIs RESTFul poderosas e escaláveis; E Bootstrap, kit de ferramentas para desenvolvimento front-end. Facilita a confecção de páginas responsivas e estilizadas de maneira fácil e rápida.

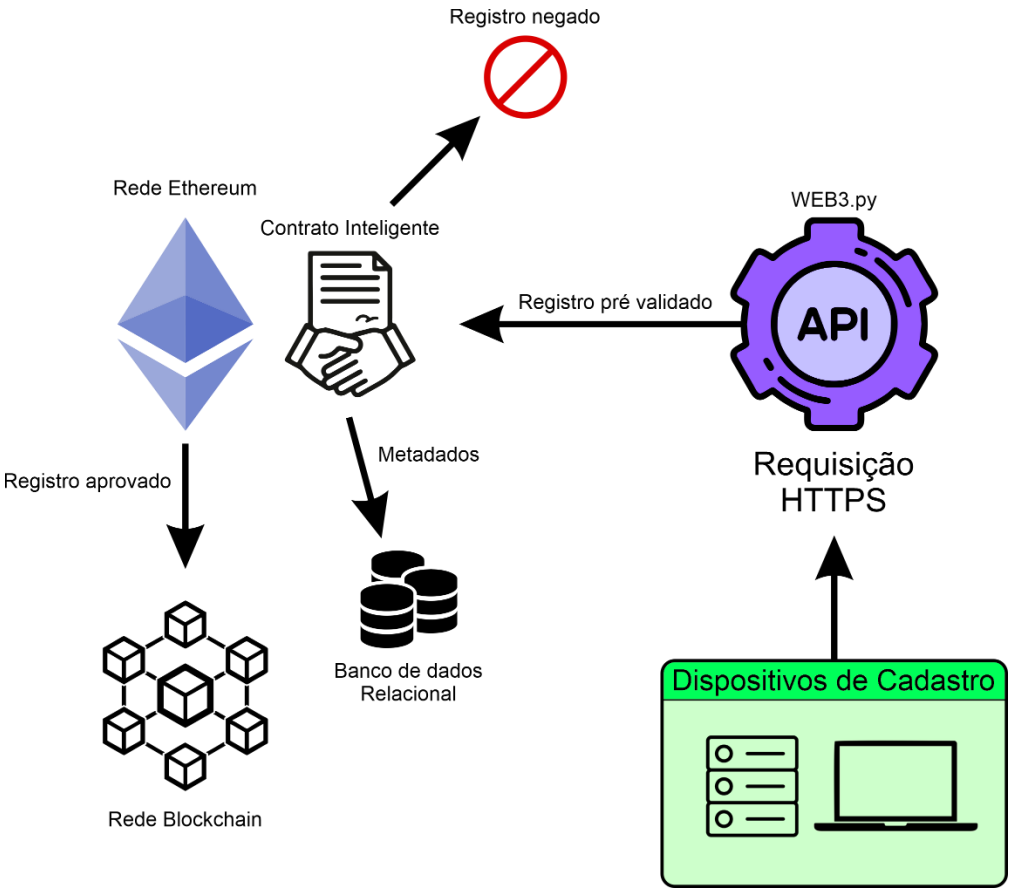
Para a realização de testes na rede foi usado a rede de teste, ou Testnet, Ethereum Sepolia, umas das principais redes de teste para a plataforma da Ethereum. Este método é usado para que contratos inteligentes sejam testados antes de serem submetidos na Mainnet (rede principal Ethereum). A rede Sepolia não possui valor monetário real, mas exige gastos de ethers falsos, chamados de faucets ethers para que suas operações sejam executadas, aproximando assim a rede de testes do mais próximo possível da rede principal. Para obter estes faucets ethers basta apenas acessar qualquer portal que faça esta emissão e fonecer o endereço da sua carteira.

Para alteração da rede Testnet para Mainnet basta mudar a variável de ambiente, colocando o endereço da rede principal, ao invés da rede de teste.

A aplicação possui um módulo backend, que funciona por meio de uma Application Programming Interface, ou API, para permitir integração a outros sistemas institucionais, e um módulo frontend, que serve tanto para testar as funcionalidades da aplicação, quanto também para uso direto da instituição e alunos.

O funcionamento da API pode ser explicada pela Figura 02:

Figura 02 – Fluxo de funcionamento da API



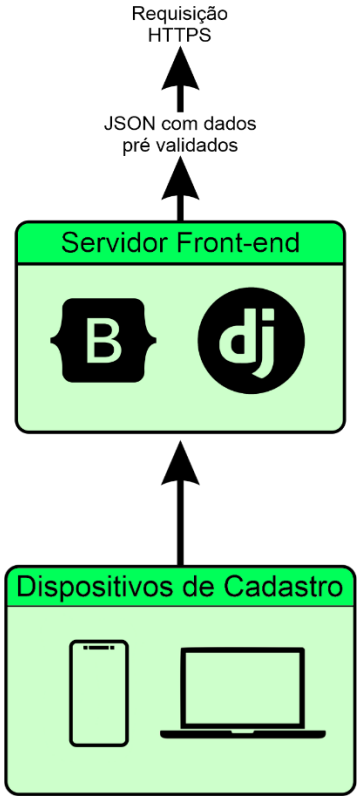
Fonte: Própria (2024).

Em resumo, um dispositivo de cadastro, consumindo a API, envia uma requisição HTTPS para a aplicação, que faz uma pré validação dos dados antes de enviar ao contrato inteligente (a fim de evitar processamento e custos desnecessários). Caso o registro seja enviado ao contrato inteligente, é avaliado a sua validade e conformidade com regras impostas. Caso tudo ocorra bem, é registrado isto na blockchain Ethereum, assim fazendo parte da rede, e enviado alguns metadados ao banco de dados da instituição. Caso contrário, o registro é simplesmente descartado.

No caso do módulo frontend, este é o seu funcionamento, explicado pela Figura 03:

Figura 03 – Fluxo de funcionamento do frontend

ISSN: 2596-0857
PREFIXO DOI: 10.31692/2596-0857



Fonte: Própria (2024).

Quando o dispositivo de cadastro se conecta ao frontend da aplicação é lhe fornecido o formulário para submissão do certificado. Ao fazer o envio acontece uma pré validação dos dados submetidos, e com tudo ocorrendo bem, é enviado o JSON com estes dados por meio de uma requisição HTTPS à API, seguindo assim o fluxo já explicado na Figura 02.

Quanto aos requisitos, ao longo de toda a aplicação ocorreram seis etapas da análise destes dados, assim, o Quadro 01 que representa os requisitos finais do software CertEthereum foram:

Quadro 01 – Requisitos Funcionais

Requisito	**Detalhes**	**Cumprido**
Consulta livre	O sistema deve permitir que qualquer pessoa, sem a necessidade de login no sistema, possa fazer a consulta de certificados.	X
Consulta geral e específica	O sistema deve permitir que o usuário possa consultar todos os certificados associados a um CPF, mas também seja possível a pesquisa de um certificado específico via hash.	X
Emissão em *blockchain*	O sistema deve emitir o certificado completo e registrá-lo na *blockchain*, sem necessidade de complemento com banco de dados local.	X
Login somente	O sistema deve permitir a criação de usuários **apenas** de	X

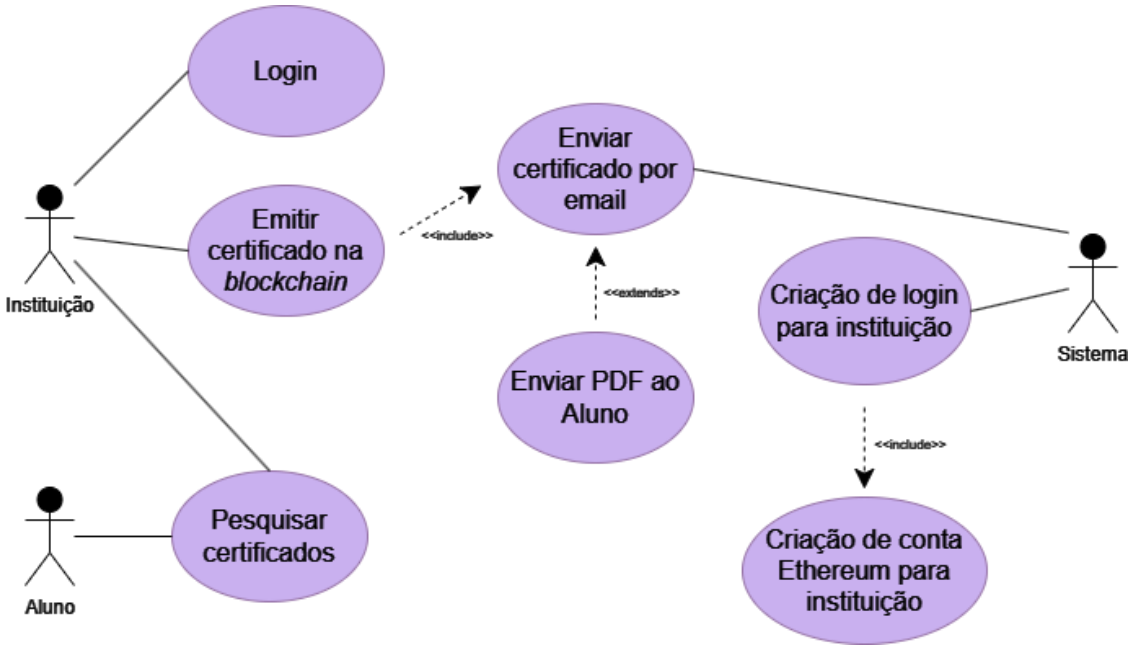
ISSN: 2596-0857
PREFIXO DOI: 10.31692/2596-0857

para Instituições	instituições de ensino, já que apenas estas iram submeter certificados.	
Envio de certificado para Email	O sistema deve enviar o certificado para o Email do aluno, com os dados mais importantes discriminados no texto do email, e a possibilidade de envio do PDF neste mesmo email.	X
Campos condizentes com realidade	A emissão de certificados deve exigir os mesmos dados, ou próximo disso, para condizer com a realidade acadêmica.	X
Geração de conta Ethereum para Instituição	Deve ser possível a geração de conta e chave privada da rede Ethereum a partir do sistema, ou código dedicado para isso.	X
Criação de *API*	O sistema deverá servir uma *API RESTful* para o consumo de módulo *frontend.*	X
Criação de *frontend* auxiliar	O sistema deverá ter um módulo *frontend* para servir de ambiente de testes, demonstração e uso real.	X

Fonte: Própria (2024).

Desta forma é possível obter o diagrama de caso de uso, como mostrado na Figura 04:

Figura 04 – Diagrama de caso de uso



Fonte: Própria (2024).

Com este diagrama é possível visualizar todas as interações que a instituição e o aluno conseguem com o sistema, além das interações automáticas do sistema.

ISSN: 2596-0857
PREFIXO DOI: 10.31692/2596-0857

Há também os requisitos não funcionais da aplicação, elucidados no Quadro 02:

Quadro 02 – Requistos não funcionais

Requisito	Detalhes	Cumprido
Segurança ponta a ponta	O sistema deve possuir os métodos de segurança recomendados para sistemas *WEB*, como *tokens JWT* e uso de protocolo *HTTPS*.	X
Tempo de resposta	O tempo de processamento de dados da API não deve passar de 01 segundo, e todo tempo adicional deve decorrer da interação com a rede Ethereum.	X
Escalabilidade	O sistema deve possuir a capacidade de escalar seu escopo sem comprometer seu desempenho.	X
Tolerância e tratamento de erros	O sistema deve ser capaz de tolerar, tratar e informar corretamente erros, obedecendo as recomendações do protocolo *HTTP*.	X
Documentação	A *API* deve possuir documentação clara e interativa, com uso de *Swagger* ou *RAML*.	X
Interface *frontend* intuitiva	A interface *frontend* deve ser intuitiva e direta, com mensagens e descrições claras.	X
Interoperabilidade da *API*	A *API* deve seguir os padrões *REST* ou *SOAP* para facilitar integrações com ferramentas de terceiros.	X

Fonte: Própria (2024).

A análise de requisitos desta aplicação ocorreu com conversas entre aluno e orientadores, conversas com servidores do IFPI – Campus Floriano e pesquisas nos materiais acadêmicos já citados. Depois da elucidação dos requisitos, a validação do cumprimento destes foi feita colhendo as devolutivas dos orientadores e em especial do coordenador de extensão do Instituto Federal, responsável pela tratativa e gerenciamento de certificados emitidos no campus.

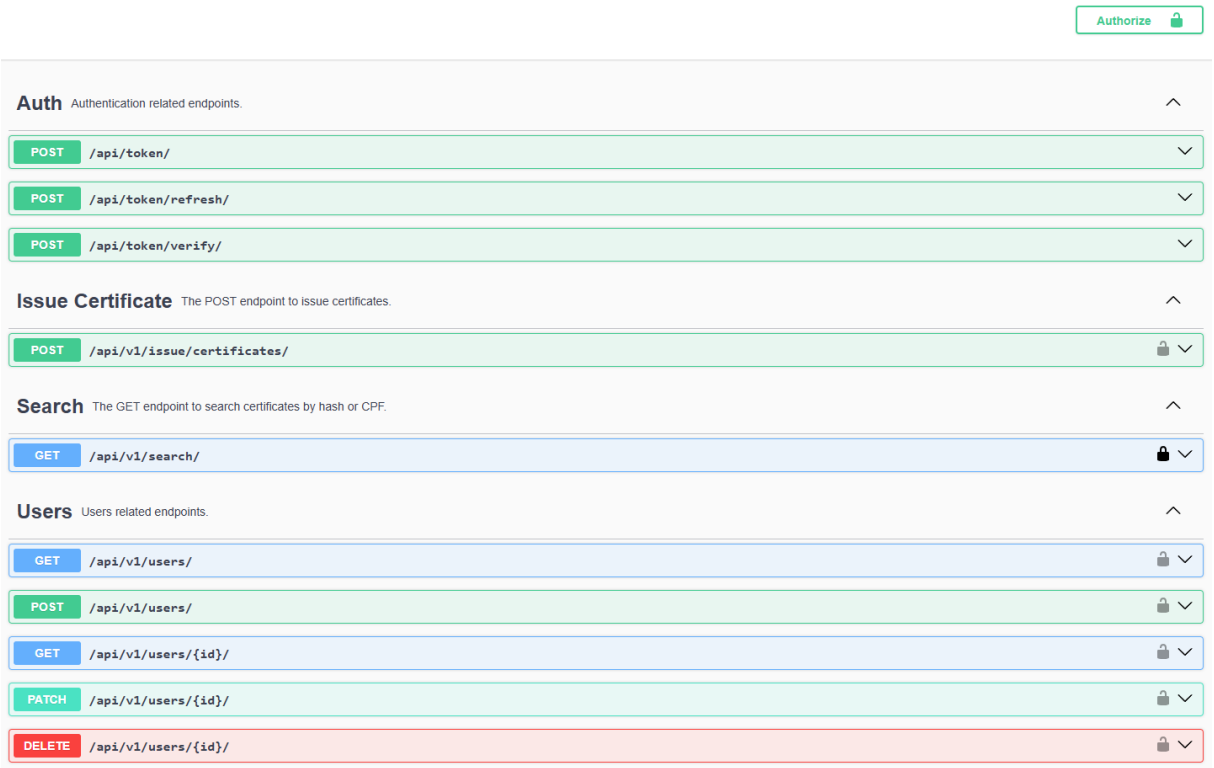
RESULTADOS E DISCUSSÃO

Considerando todo o apresentado, esta seção tem seu foco em mostrar o software CertEthereum em seu resultado final.

O módulo que serve a API deste projeto foi desenvolvido desde o começo com foco em sua acessibilidade e facilidade de uso, seguindo os padrões REST, inclusive na nomeação de

cada endpoint, usando também documentação interativa Swagger, sendo esta a documentação gerada:

Figura 05 – Endpoints da API



Fonte: Própria (2024).

A figura acima demonstra todos os *endpoints* disponíveis na *API*, que se dividem em categorias por ordem alfabética:

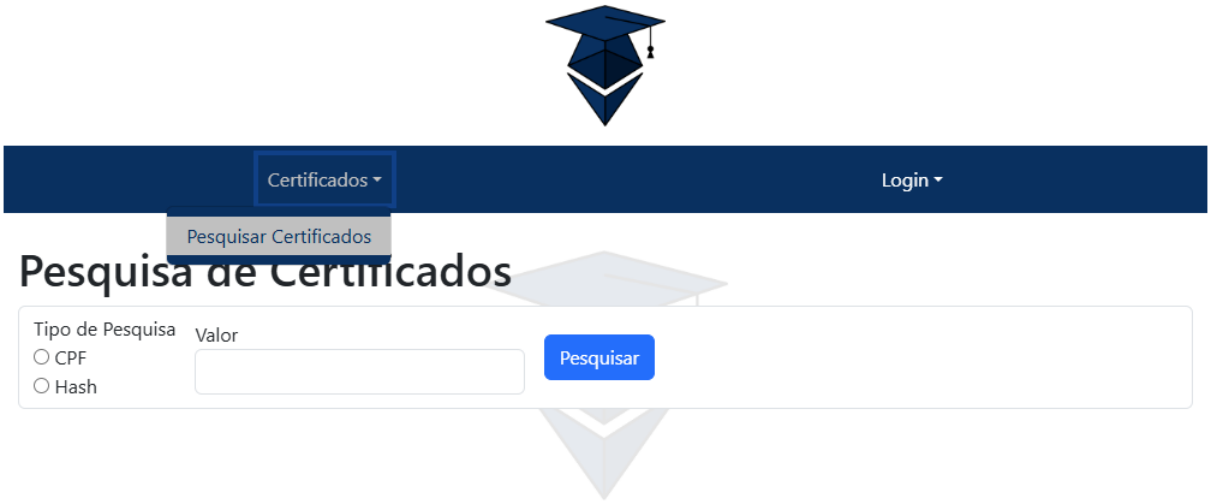
1) "*Auth*": têm como objetivo tratar das funções específicas de autenticação no sistema (obtenção de *token* de login, atualização de *token* e verificação de validade dele). **2) "*Issue Certificate*":** é a rota de submissão de certificado, responsável por receber os dados do certificado e inseri-lo na rede *blockchain*, retornando o resultado desta operação normalmente entre 5 e 8 segundos, que é o tempo médio percebido pelos autores que a transação é processada e validada. **3) "*Search*":** é usada na pesquisa de certificados por CPF ou *hash*. **4) "*Users*":** agrupa as rotas do *CRUD* completo para os dados dos usuários (instituições).

É importante esclarecer que para a aplicação rodar com todas as suas funcionalidades, as variáveis de ambiente devem estar bem configuradas em um arquivo ".env" na raiz do projeto. As variáveis a serem configuras são as seguintes estão listadas na documentação do repositório deste projeto.

O módulo de *frontend* desta aplicação foi pensado para ser o mais direto possível, principalmente para que usuários leigos consigam usar sem grandes problemas.

Abaixo está a tela de pesquisa de certificados, que pode ser acessada pela instituição, aluno ou interessados nestes dados:

Figura 06 – Tela de pesquisa de certificados

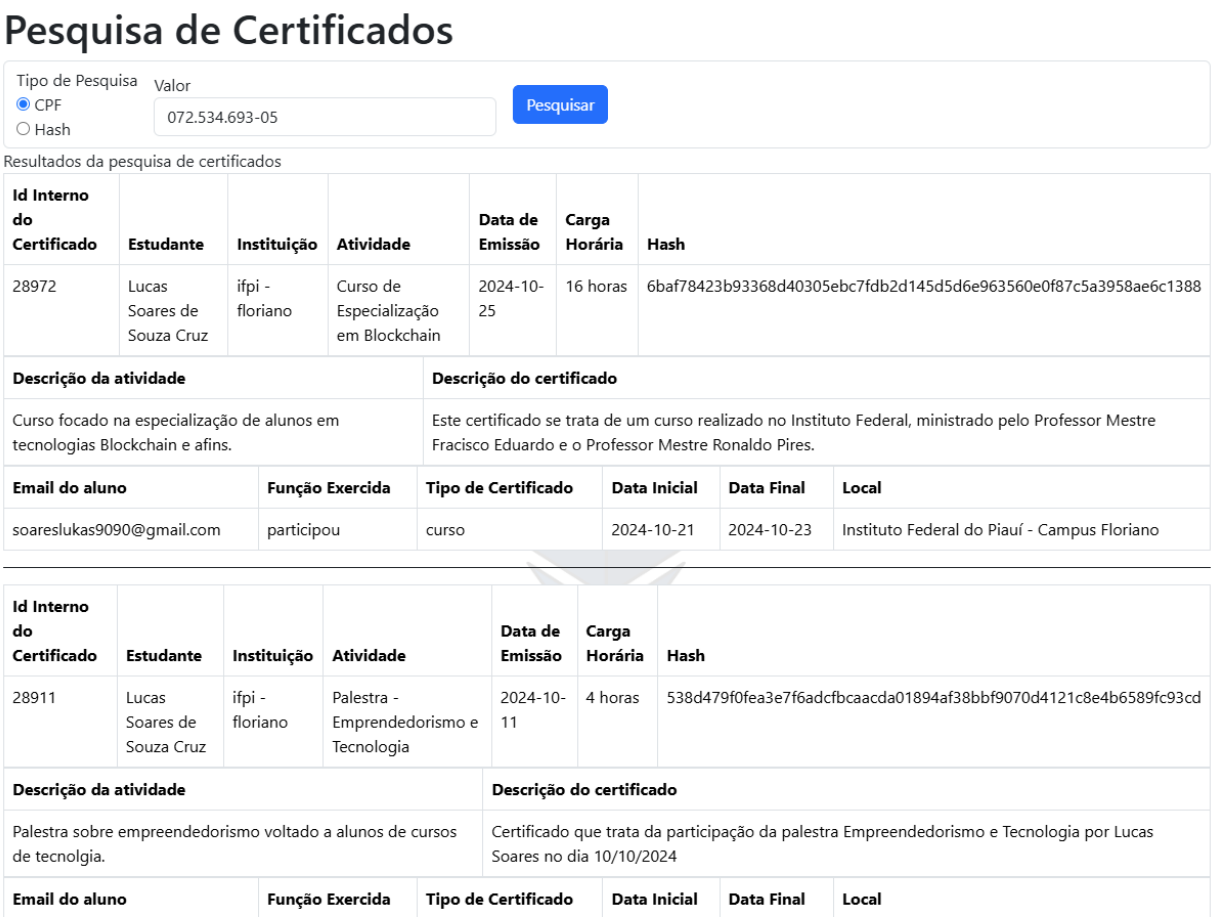


Fonte: Própria (2024).

O submenu de Certificados oferece apenas a opção de Pesquisar Certificados no caso de usuários deslogados. Na tela que vem por consequência é possível a pesquisa por CPF e por hash, havendo duas diferenças entre elas: A primeira é que a pesquisa por CPF permite 0 a vários resultados, por vários certificados podem estar associados a um CPF, mas a pesquisa por hash traz 0 ou 1 resultado, pois não é possível que dois ou mais certificados possuam o mesmo valor de hash. A segunda diferença é menor, porém importante para a experiência de usabilidade do usuário, pois ao selecionar CPF é aplicado um filtro de auto formatação de CPFs no campo e pesquisa.

Abaixo está um exemplo de pesquisa de certificado por CPF com retorno válido:

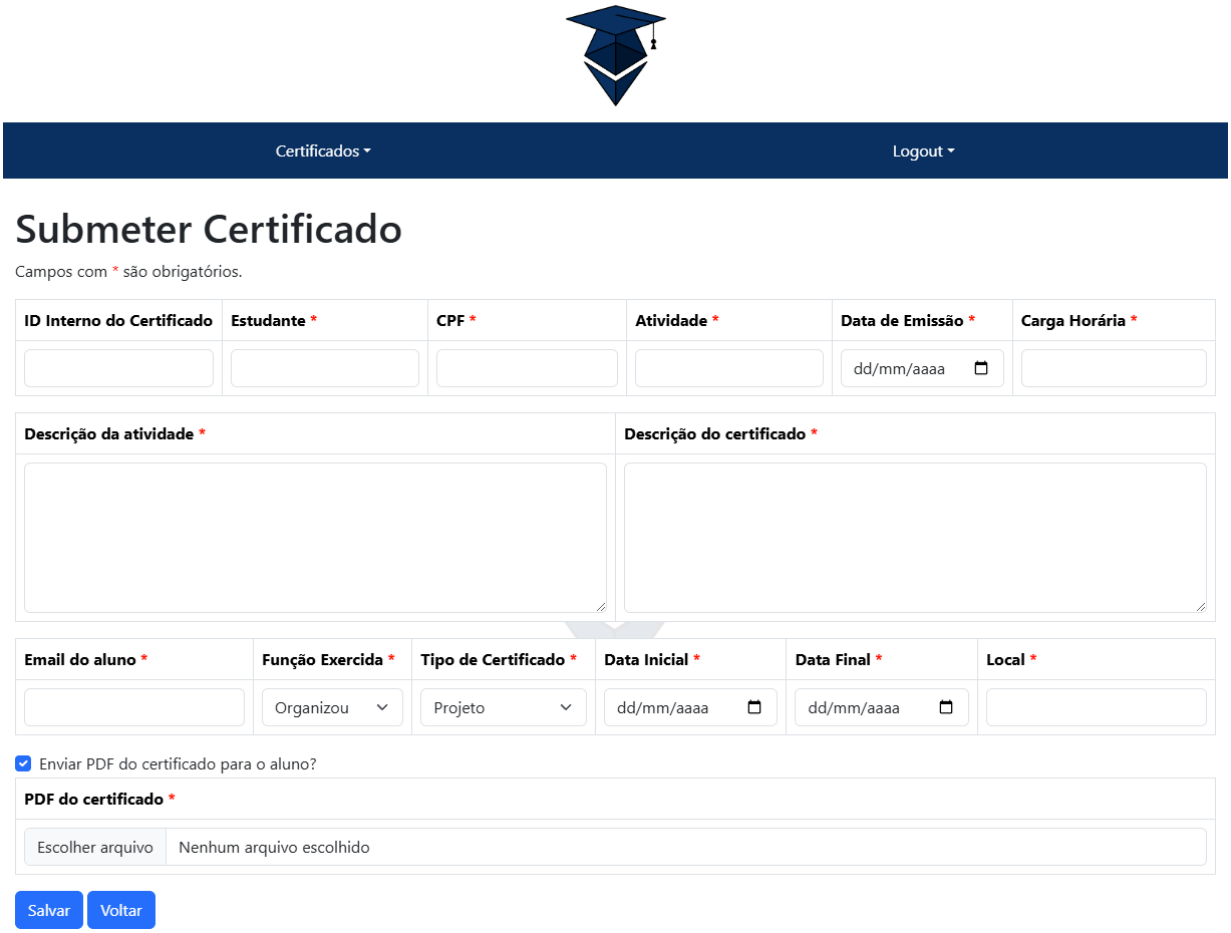
Figura 07 – Listagem de certificados associados a um CPF



Fonte: Própria (2024).

Já para instituições logadas no sistema, o menu Certificados oferece também a opção de inserção de certificados. Esta inserção já é feita diretamente na rede *blockchain*. A página também conta com um *checkbox* que registra o objetivo ou não de enviar algum arquivo referente ao certificado junto ao email que será enviado ao aluno. É importante entender que com esta *checkbox* marcada a submissão do certificado só é possível ao selecionar algum arquivo.

Figura 08 – Tela de submissão de certificados



Fonte: Própria (2024).

O único campo não obrigatório na submissão é o “ID interno do Certificado”, pois este campo se destina a guardar a identidade do certificado no banco de dados interno da instituição.

Após a submissão do certificado é retornado a mensagem informando o sucesso, ou erro se for o caso. Caso a resposta seja positiva, é retornado também o *hash* do certificado e enviado o email com estes dados para o aluno.

CONCLUSÕES

Este trabalho explorou o desenvolvimento de uma aplicação para armazenamento e validação de certificados acadêmicos utilizando a tecnologia blockchain. Desde a fundamentação teórica sobre os benefícios e desafios da blockchain até a implementação de uma solução prática com a rede Ethereum e contratos inteligentes, buscamos responder à questão de viabilidade e eficácia deste modelo para o sistema educacional brasileiro.

A análise e os resultados obtidos demonstram que o uso de blockchain na emissão de certificados oferece uma solução robusta para questões de autenticidade, imutabilidade e acessibilidade de dados acadêmicos. Ao garantir que esses registros são verificados e imutáveis,

a aplicação agrega confiabilidade e facilita o acesso, proporcionando uma nova forma de controle e autonomia para os estudantes em relação aos seus dados acadêmicos.

Mesmo com as vantagens obtidas, tanto para alunos, quanto para instituições, sejam relevantes, é importante considerar os desafios que certamente serão enfrentados à tentativa de implantação e uso contínuo desta ferramenta.

O modelo deste *software* sofre de algumas desvantagens, decorrentes da sua natureza de uso de uma *blockchain* de terceiros. É possível listar os seguintes:

- **Imutabilidade**: Uma das principais vantagens do modelo também pode ser um de seus principais problemas. Caso qualquer certificado errado seja carregado à rede, este permanecerá como um dos registros da *blockchain* independente de tentativas de correções. Um dos motivos pelo qual foi escolhido o *design* de *API* para esta aplicação foi a possibilidade de integração com sistemas de gerenciamento educacional já existentes, desta forma dados como nome, CPF, atividade, entre outros, teriam uma menor probabilidade de serem submetidos de forma errônea, pois eliminaria o fator humano da questão.
- **Preço**: Talvez a principal desvantagem, o preço do uso dos recursos da *blockchain* Ethereum pode ser um problema desanimador, já que o uso de *gas* não é fixo, pois depende do congestionamento da rede, e a cotação da moeda Ethereum está atualmente com valor muito alto frente ao real brasileiro. Uma possível solução para isso seria a escolha do aluno entre emitir seu certificado na *blockchain* ou não, e o repasse de parte ou de todo o custo para ele. Outra via seria a utilização de outra rede *blockchain*, como a Solana, que possui custo muito menores, já que é voltada para a execução de *Dapps*.
- **Complexidade técnica**: Implementar e gerenciar a tecnologia seria com certeza um ponto desagradável. O mercado *blockchain* possui alta volatilidade, além de estar em constante evolução, assim o código do contrato inteligente deveria sempre estar atualizado, para corresponder a mudanças e atualização na rede. Isso exigiria também um bom versionamento de código e contratos, pois certificados emitidos por um certo contrato deveriam ser possibilitados de serem encontrados por certificados mais “novos”. Este percalço pode ser ultrapassado com a capacitação dos profissionais desenvolvedores que iram manter o sistema.
- **Privacidade e LGPD**: A Lei Geral de Proteção de Dados do Brasil estabelece o direito ao esquecimento, no qual um aluno poderia pedir para que um registro seu não fosse acessível ao público, o que é impedido pela natureza imutável desta rede. Para contornar isso, o CertEthereum usa o CPF do aluno apenas para indexação, não sendo possível a

recuperação deste dado ao buscar por um certificado. Porém, mesmo desta forma, é preciso uma análise mais profunda para garantir a conformidade com a lei.

Considerando todo o apresentado, este trabalho pode ter seu escopo evoluído. Buscando a integração deste sistema a outras aplicações já existentes, a fim de alimentar a entrada de dados com informação já validadas e guardadas em um banco de dados de uma instituição. Pode-se servir também para estudos e base para implementação de *blockchain* para mais que apenas certificados, mas outros documentos.

Outros recursos conhecidos da tecnologia *blockchain* também podem ser considerados, como os *Non Fungible Token* (NFT). Além disso, *blockchains* privadas podem representar um grande avanço para os rumos deste trabalho, pois a segurança e privacidade com certeza seriam aumentadas.

Embora os desafios técnicos e econômicos, como o custo de processamento e a curva de aprendizado para adaptação da tecnologia, sejam fatores relevantes a serem considerados, este projeto valida que a aplicação de blockchain na educação possui grande potencial. A criação do CertEthereum é um passo promissor em direção a um modelo mais seguro, descentralizado e eficiente para o gerenciamento de registros acadêmicos.

Por fim, acredita-se que o presente trabalho contribui tanto para a academia quanto para a sociedade, oferecendo uma visão prática de como a tecnologia blockchain pode revolucionar a gestão de documentos acadêmicos. Sugere-se, para pesquisas futuras, o aprofundamento em questões de escalabilidade, integração com outras redes blockchain e aprimoramento de mecanismos de segurança e privacidade, visando o aperfeiçoamento contínuo deste modelo.

ISSN: 2596-0857
PREFIXO DOI: 10.31692/2596-0857

REFERÊNCIAS

Agencia de Noticia U. N., Colombia.com. 2019.

AHLUWALIA, Saurabh; MAHTO, Raj V.; GUERRERO, Maribel. Blockchain technology and startup financing: A transaction cost economics perspective. **Technological Forecasting and Social Change**, v. 151, p. 119854, 2020.

ASIF, Rameez; HASSAN, Syed Raheel. Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. **Frontiers in Blockchain**, v. 6, p. 1151724, 2023.

BUTERIN, Vitalik et al. A next-generation smart contract and decentralized application platform. **Ethereum White Paper**, v. 3, n. 37, p. 2-1, 2014.

CASSEZ, Franck; FULLER, Joanne; ASGAONKAR, Aditya. Formal verification of the ethereum 2.0 beacon chain. In: **International Conference on Tools and Algorithms for the Construction and Analysis of Systems**. Cham: Springer International Publishing, 2022. p. 167-182.

CRUZ, J. C. et al. Tecnologia Blockchain: um novo paradigma nas ciências abertas. **ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO**, v. 19, 2018.
FAROKHNIA, Soroush; GOHARSHADY, Amir Kafshdar. Reducing the gas usage of Ethereum smart contracts without a sidechain. In: **2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)**. IEEE, p. 1-3, 2023.

GUPTA, Suyash; SADOGHI, Mohammad. Blockchain transaction processing. **arXiv preprint arXiv:2107.11592**, 2021.

JAIN, Archana; JAIN, Chinmay. Blockchain hysteria: Adding “blockchain” to company’s name. **Economics Letters**, v. 181, p. 178-181, 2019.

JIRGENSONS, Merija; KAPENIEKS, Jānis. Blockchain and the future of digital learning credential assessment and management. **Journal of teacher education for sustainability**, v. 20, n. 1, p. 145-156, 2018.

KASTENSSON FAN, Daniel. A Blockchain-Based Solution to High-Volume Web Scraping With Smart Contracts on Ethereum. 2018.

KHAN, Shafaq Naheed et al. Blockchain smart contracts: Applications, challenges, and future trends. **Peer-to-peer Networking and Applications**, v. 14, p. 2901-2925, 2021.

KOUTMOS, Dimitrios. Network activity and ethereum gas prices. **Journal of Risk and Financial Management**, v. 16, n. 10, p. 431, 2023.

LASHKARI, Bahareh; MUSILEK, Petr. A comprehensive review of blockchain consensus mechanisms. **IEEE access**, v. 9, p. 43620-43652, 2021.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.

NARAYANAN, Arvind et al. **Bitcoin and cryptocurrency technologies: a comprehensive introduction**. Princeton University Press, 2016.

RAMÍREZ, Juan Pablo Valencia. Contratos inteligentes. **Revista de Investigación en Tecnologías de la Información**, v. 7, n. 14, p. 1-10, 2019.

SELNER, Claudiomir et al. Análise de requisitos para sistemas de informações, utilizando as ferramentas da qualidade e processos de software. 1999.

SIFAH, Emmanuel Boateng et al. BEMPAS: a decentralized employee performance assessment system based on blockchain for smart city governance. **IEEE Access**, v. 8, p. 99528-99539, 2020.

SOMMERVILLE, Ian. Software Engineering, 9. ed. **England: Education Limited**, 2010.

TA, Minh Thanh; DO, Tien Quyet. A study on gas cost of ethereum smart contracts and performance of blockchain on simulation tool. **Peer-to-Peer Networking and Applications**, v. 17, n. 1, p. 200-212, 2024.

WAINER, Jacques et al. Métodos de pesquisa quantitativa e qualitativa para a Ciência da Computação. **Atualização em informática**, v. 1, n. 221-262, p. 32-33, 2007.

ZHENG, Zibin et al. An overview on smart contracts: Challenges, advances and platforms. **Future Generation Computer Systems**, v. 105, p. 475-491, 2020.