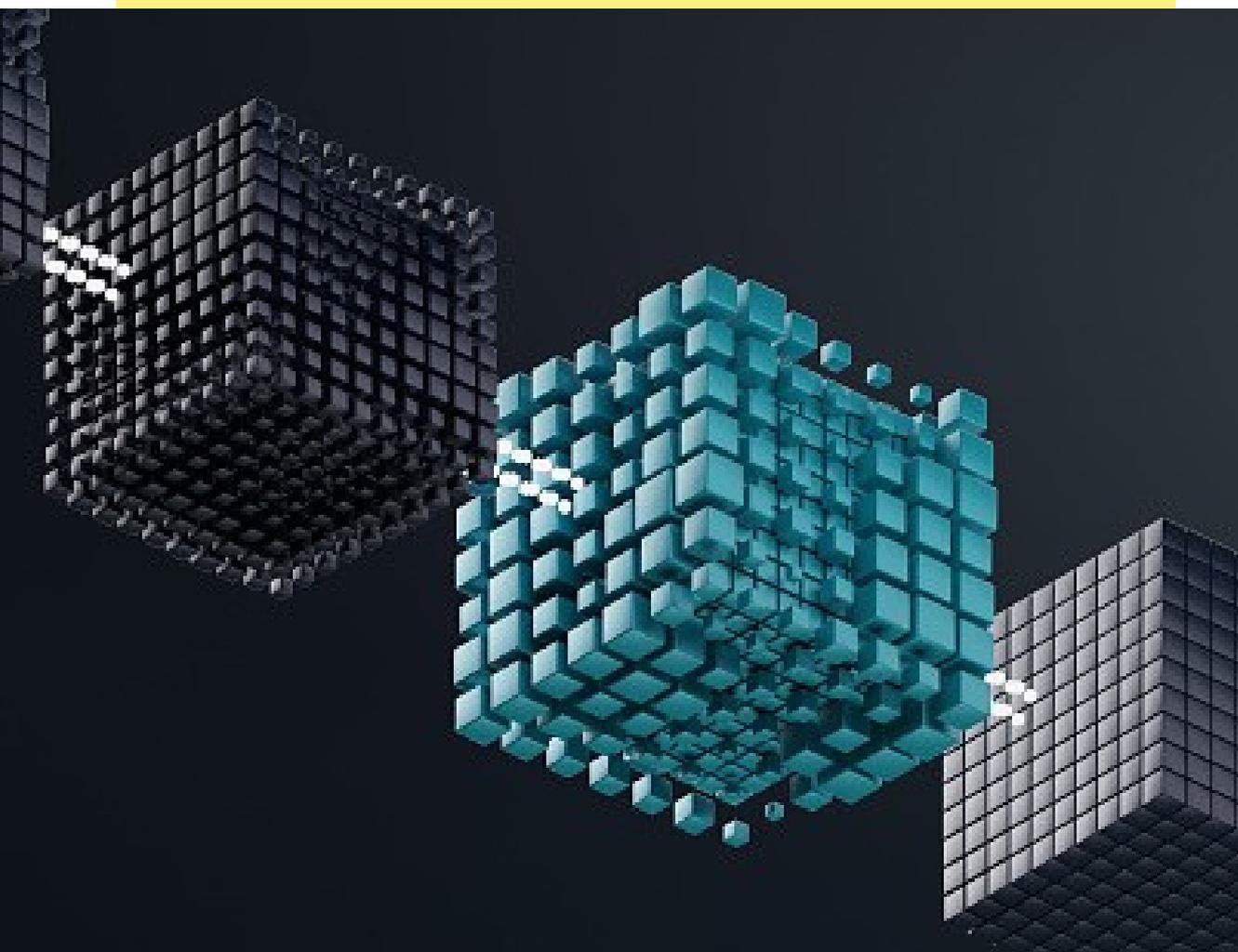


# APLIVATIVO PARA ENVIO DE DADOS A BLOCKCHAIN

RELATÓRIO TÉCNICO & INSTRUÇÕES DE IMPLEMENTAÇÃO



# SUMÁRIO

---

<b>01.</b> Resumo .....	3
<b>02.</b> Contexto .....	4
<b>03.</b> Público-alvo .....	4
<b>04.</b> Descrição da Situação-Problema .....	5
<b>05.</b> Objetivos da proposta .....	6
<b>06.</b> Análise da situação-problema .....	7
<b>07.</b> Proposta de Intervenção .....	8
<b>08.</b> Responsáveis .....	9

---

# RESUMO



A tecnologia blockchain tem sido cada vez mais mencionada pelo Governo Federal como uma possível ferramenta para modernizar e aperfeiçoar os processos na esfera pública. Essa tecnologia pode ser compreendida como um registro distribuído capaz de garantir a imutabilidade e autenticidade de dados, sem depender de uma autoridade central, e é considerada por muitos autores como uma tecnologia disruptiva, capaz de gerar inovação ao romper com modelos antigos e introduzir novos padrões. Impulsionado por essas premissas, foi proposto e executado, o desenvolvimento uma aplicação que utiliza a blockchain da rede Ethereum para assegurar a imutabilidade, integridade e disponibilidade de um item do acervo acadêmico originado de uma Instituição Federal de Ensino Superior (IFES), mas que pode ser utilizada para o envio de qualquer tipo de documento. Em nossa proposta utilizamos a aplicação *back-end* desenvolvida pelo autor para enviar à blockchain um comprovante de matrícula gerado pelo aplicativo móvel para estudantes e servidores desenvolvido pelo Instituto de Ciências Exatas (ICE) da Universidade Federal de Juiz de Fora (UFJF).

*A adoção da tecnologia blockchain poderia ser usada para garantir uma gestão pública mais segura e prática (PORTAL TCU, 2020)*

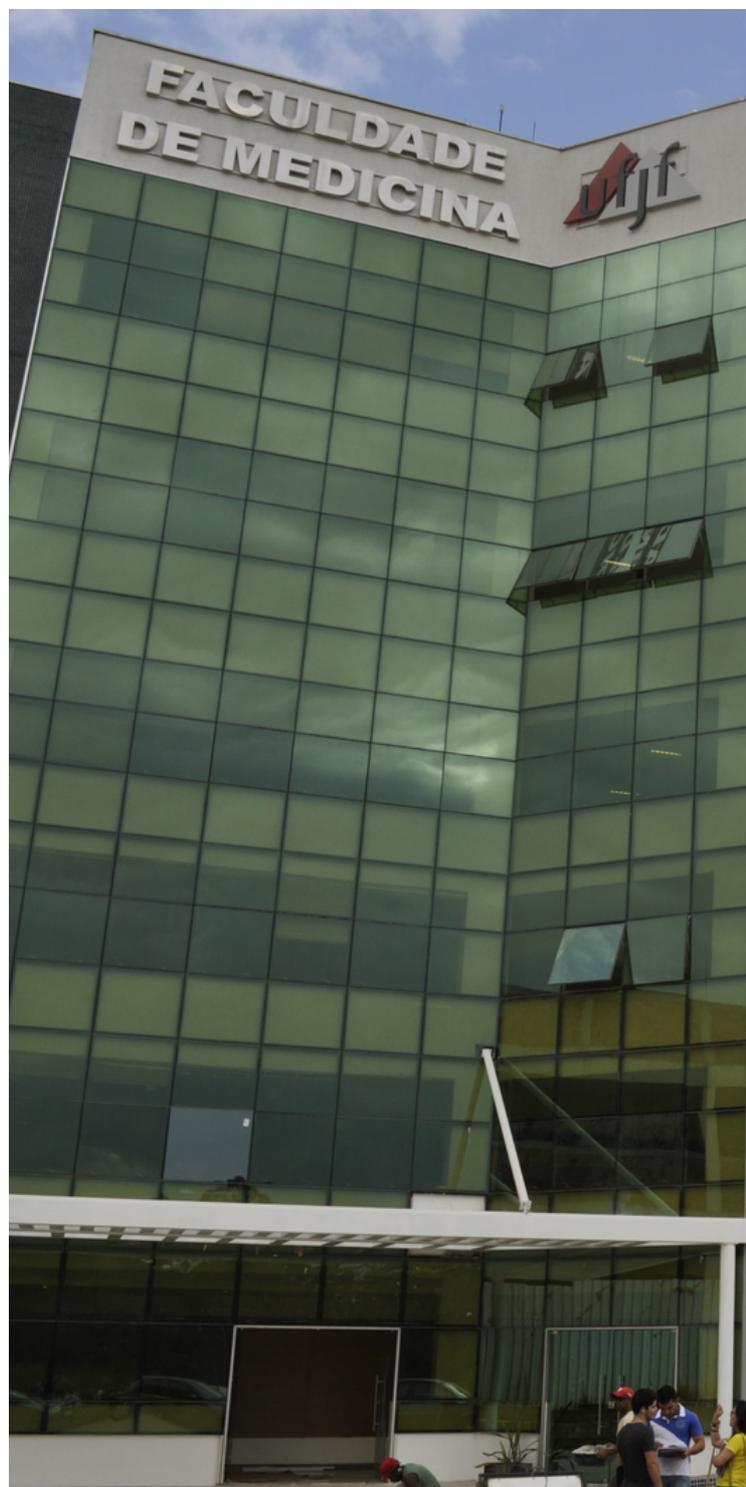
# CONTEXTO

A proposta de intervenção foi concebida no ICE da UFJF durante o desenvolvimento do aplicativo que será utilizado para fornecer serviços aos alunos e servidores da unidade.

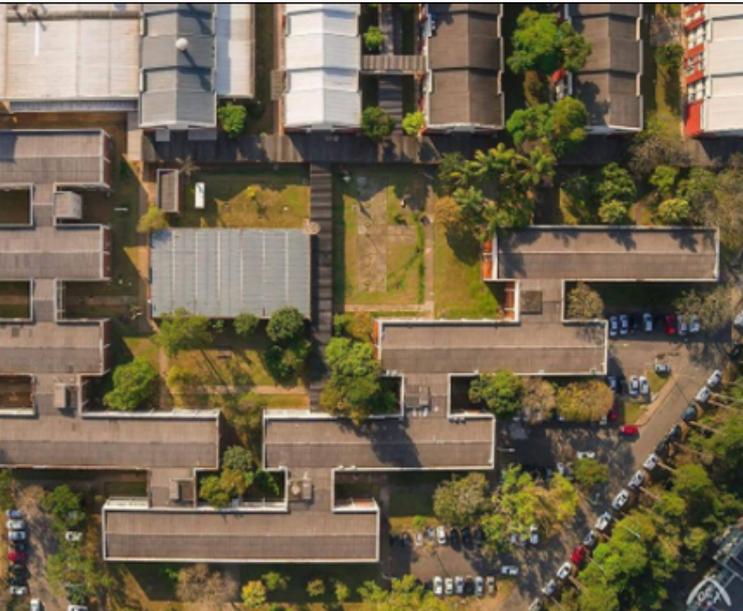
Pautada no estímulo feito pelo MEC, na busca de novas tecnologias para a gestão de documentos como diplomas e certificados (MEC, 2022), além das iniciativas do Governo Federal, ligadas ao desenvolvimentos de estudos e aplicações utilizando a tecnologia blockchain (TCU, 2022), a idéia de desenvolvimento de uma solução capaz de unir esses dois temas surgiu.

## PÚBLICO ALVO

A implementação da ferramenta “aplicação back-end para envio de documentos à blockchain” pode beneficiar de forma direta alunos e usuários externos à comunidade acadêmica. A utilização de uma rede blockchain para armazenar documentos oficiais como comprovantes de matrículas, certificados e diplomas, representa uma série de vantagens quando comparado aos métodos tradicionais, essas vantagens serão apresentadas nos próximos tópicos público alvo



# DESCRIÇÃO DA SITUAÇÃO-PROBLEMA



Emitir e consultar a autenticidade de um documento ou diploma é um processo por vezes custoso e lento. Utilizando um exemplo específico: alunos ou empregadores que estão no exterior e que precisam verificar a validade de um diploma, seja para a admissão em um cargo de trabalho, ou seja para um processo seletivo, devem requerer uma tradução e posteriormente a autenticação e legalização, dessa tradução, geralmente através de um serviço notarial pago, como medida para provar a autenticidade dos seus documentos. Porém, com os recentes avanços ligados a ciências da computação e com o desenvolvimento da tecnologia blockchain, dotada de características como imutabilidade, descentralização, segurança e rastreabilidade, a sua adoção pode ser uma excelente escolha que vai de encontro às necessidades de incremento dos aspectos de segurança e acessibilidade, permitindo que um diploma ou documento possa ser verificado por qualquer parte interessada, a partir de qualquer lugar do globo, sem a necessidade de um intermediário ou de uma autoridade certificadora (CASTRO,2021).

*"A tecnologia blockchain pode aumentar a eficiência e transparência de sistemas governamentais." (WEF, 2021)*

# OBJETIVOS

Através do desenvolvimento e implementação de aplicação que utiliza a blockchain Ethereum para assegurar a imutabilidade, garantir a integridade, autenticidade e disponibilidade de um documento nato-digital, originado de uma IFES, pretendemos atingir os seguintes objetivos específicos:

- 01.** Possibilitar a submissão de um documento do acervo acadêmico à blockchain da rede Ethereum.
- 02.** Possibilitar o acesso ao documento por qualquer cidadão ou instituição quando se fizer necessário
- 03.** Permitir o armazenamento de forma descentralizada e distribuída, diminuindo assim a incidência de eventos adversos ligados a perda de dados
- 04.** Diminuir a incidência de fraudes se valendo da característica de imutabilidade inerente à tecnologia blockchain.
- 05.** Criar um modelo de segurança capaz de ser reproduzido e aperfeiçoado por outras instituições

# DIAGNÓSTICO E ANÁLISE DA SITUAÇÃO-PROBLEMA

Os esforços feitos pelo MEC na construção de parâmetros mais maduros e seguros para a emissão do acervo acadêmico pelas IFES, são claramente um passo para a consolidação de uma estrutura mais sólida no combate às fraudes, mas alguns pontos continuam de certa forma descobertos.

De acordo com Lepiane *et al*, (2019), mesmo após mudanças recentes na questão da emissão e autenticação de itens do acervo acadêmico, a natureza distribuída do processo ainda persiste, já que cada Instituição deve manter um repositório com os dados de cada documento, essas informações ainda estão suscetíveis a incidentes técnicos ou a desastres naturais que podem causar perda de dados. Um outro detalhe ainda presente é a presença de uma autoridade central certificadora, intermediando o processo, o tornando mais burocrático e dependente. Porém, com o desenvolvimento da tecnologia blockchain, dotada de características como imutabilidade, descentralização, segurança e rastreabilidade, a sua adoção pode ser uma excelente escolha que vai de encontro às necessidades de incremento dos aspectos de segurança e acessibilidade, permitindo que um diploma ou documento possa ser verificado por qualquer parte interessada, a partir de qualquer lugar do globo, sem a necessidade de um intermediário ou de uma autoridade certificadora (CASTRO,2021).

Frente ao exposto, entendemos que desenvolver meios para aumentar a segurança, facilitar a autenticidade e disponibilidade de documentos que fazem parte do acervo acadêmico emitidos por IFES, através do desenvolvimento de soluções tecnológicas como, softwares, aplicativos ou outros tipos de sistemas informatizados que adotam a tecnologia blockchain como estrutura de armazenamento e distribuição de dados, é um senso comum por parte do governo federal, e a necessidade de modelos de confiança que possam ser desenvolvidos e utilizados como ferramentas práticas de estudo também é uma realidade



# OBJETIVOS DA PROPOSTA

Nosso objetivo é garantir e assegurar a imutabilidade, integridade e disponibilidade de um item do acervo acadêmico, utilizando a tecnologia blockchain e conforme apresentado nos tópicos anteriores, para atingir este objetivo a nossa proposta de intervenção se apresenta através da construção e implementação de um sistema back-end. Back-ends, são sistemas que não interagem diretamente com os usuários, eles são integrados a outros sistemas que são responsáveis por “conversar” com o usuário final. O diagrama apresentado na figura X, apresenta um pouco dessa dinâmica.

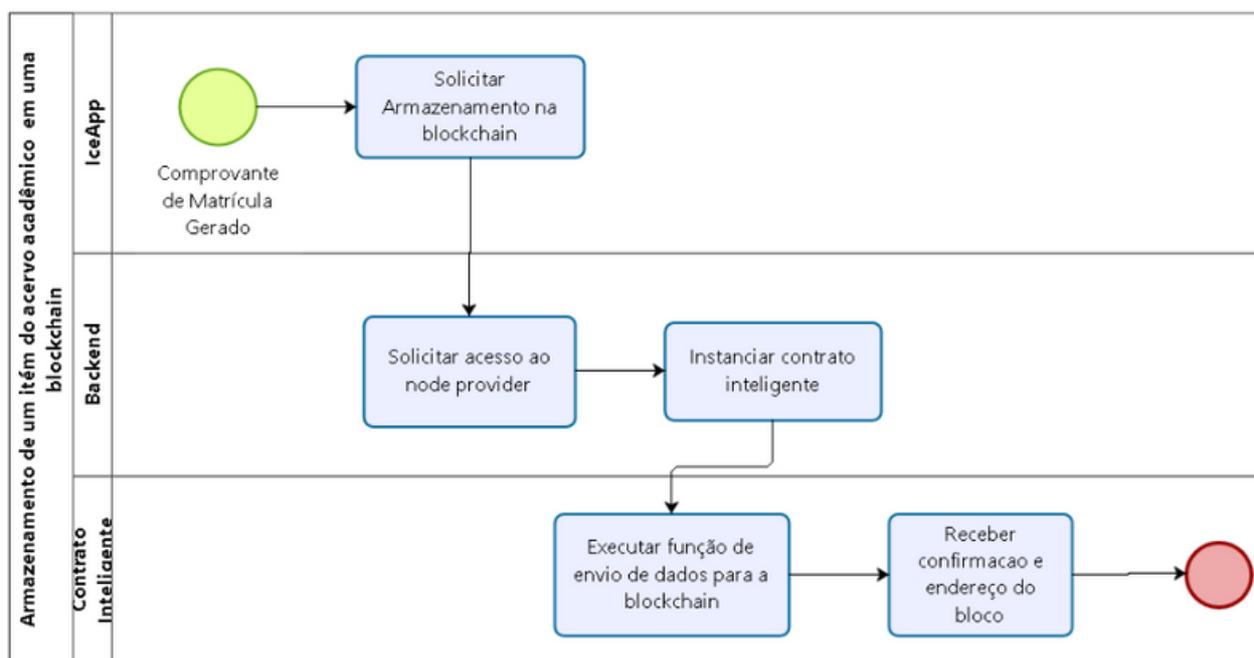
Vamos nos valer dos recursos do 5W2H, para que possamos entender melhor como implementar a nossa proposta de Intervenção

- **O que (What) ?** Realizar a implementação do nosso sistema back-end
- **Quem (Who) ?** Técnicos e analistas de TI.
- **Onde (Where) ?** Qualquer instituição pública.
- **Quando (When) ?** Após a criação de contrato inteligente e da obtenção das credenciais necessárias.
- **Porque (Por que) ?** Para garantir e assegurar a imutabilidade, integridade e disponibilidade de um item do acervo acadêmico, utilizando a tecnologia blockchain
- **Como (How) ?** Através de codificação necessária à integração, entre o back-end e a interface previamente existente
- **Quanto (How much) ?** Nenhum custo.

Conforme demonstrado no figura 5W2H, e nos parágrafos anteriores, nosso back-end, precisa ser conectado a outra aplicação ou sistema que faça a interação com o usuário final. E essa integração precisa ser construída por técnicos ou analistas de TI, com alguma experiência na área de integração de sistemas. Portanto as próximas instruções serão direcionadas a esse grupo de profissionais.

# INFORMAÇÕES TÉCNICAS PARA A INTEGRAÇÃO

Na figura abaixo, podemos observar a dinâmica de funcionamento do nosso artefato integrado a um sistema de interface já existente (ICEapp)



URL do projeto no GitHub

<https://github.com/thiagom10/backendDocToEthereum.git>

---

## **A seguir serão listadas informações e instruções importantes aos integradores que irão utilizar o back-end.**

O Sistema back-end foi construído em linguagem PHP, e possui apenas uma dependência, o pacote web3, conhecido como simple-web3-php, as informações são enviadas a ele através de requisições do tipo GET, mas podem ser facilmente substituídas por requisições POST.

Não existe qualquer camada de autenticação no nosso código, portanto, é importante que ele seja implementado junto a algum tipo de sistema de autenticação como por exemplo: Oauth 2.0.

Toda a comunicação é feito através do Node Provider Infura, por tanto é necessário que a instituição possua uma conta no serviço. Todo projeto foi constituído para utilizar o Infura. Portanto uma inegração com outro Node Provider ou mesmo diretamente a um nó da rede é possível mas vai requerer conhecimento técnico especializado e algum tempo para que seja realizado a alteração no código.

Por fim, as variáveis contendo informações essenciais precisam ser setadas, elas se encontram nas parte inicial do código fonte e são as seguintes:

- 1.Hash referente a conta/carteira virtual da instituição
- 2.Hash referente à instância do smart contratct
- 3.Chave de acesso a carteira da instituição
- 4.Credenciais de acesso ao infura.

# RESPONSÁVEIS

## **Thiago Marques Fernandes de Mello**

Bacharel em sistemas de Computação, Pós-graduado em Redes de Computadores

Servidor Técnico Administrativo na universidade Federal de Juiz de Fora, no cargo de Analista de Tecnologia da Informação

E-mail: thiago.marques@ice.ufjf.br

## **Marcos Tanure Sanábio**

Graduado em Administração, Mestre em Administração Pública, Doutor em Administração

Docente do Programa do Mestrado Profissional em

Administração Pública da Universidade Federal de Juiz de Fora

**ELABORADO EM 27/07/2023**

# REFERÊNCIAS

CASTRO, Renato Q.; AU-YONG-OLIVEIRA, Manuel. Blockchain and higher education diplomas. European Journal of Investigation in Health, Psychology and Education, v. 11, n. 1, p. 154-167, 2021.

LEPIANE, Cristiane Dias et al. Digital Degree Certificates for Higher Education in Brazil: A Technical Policy Specification. In: Proceedings of the ACM Symposium on Document Engineering 2019. 2019. p. 1-10

TCU. Rede Blockchain Brasil vai garantir mais segurança a atos e contratos públicos | Portal TCU. 05 de maio de 2022. Disponível em: <<https://portal.tcu.gov.br/imprensa/noticias/rede-blockchain-brasil-vai-garantir-mais-seguranca-a-atos-e-contratos-publicos.htm>>. Acesso em: 14 jul. 2022.

WEF. Blockchain could dismantle corruption in government services. 2021. Disponível em: <<https://www.weforum.org/agenda/2021/07/blockchain-for-government-systems-anti-corruption/#:~:text=Blockchain%20could%20improve%20the%20transparency>>