



UNIVERSIDADE FEDERAL DE SANTA CATARINA  
CENTRO TECNOLÓGICO  
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA  
SISTEMAS DE INFORMAÇÃO

Brenno Araujo Queiroz

**Badges como ferramenta de gamificação no contexto do ensino superior por  
meio de tokenização**

Florianópolis  
2023

Brenno Araujo Queiroz

**Badges como ferramenta de gamificação no contexto do ensino superior por meio de tokenização**

Trabalho de Conclusão de Curso de Graduação em Sistemas de Informação do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Johann Westphall, Me.

Coorientador: Prof. Jean Everson Martina, Dr.

Florianópolis

2023

Brenno Araujo Queiroz

**Badges como ferramenta de gamificação no contexto do ensino superior por meio de tokenização**

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de “Bacharel em Sistemas de Informação” e aprovado em sua forma final pelo Curso de Graduação em Sistemas de Informação.

Florianópolis, 5 de Dezembro de 2023.

**Banca Examinadora:**

---

Johann Westphall, Me.  
Universidade Federal de Santa Catarina

---

Prof. Jean Everson Martina, Dr.  
Universidade Federal de Santa Catarina

---

Maurício de Vasconcelos Barros, Bel.  
Universidade Federal de Santa Catarina

---

Lucas Machado da Palma, Me.  
Universidade Federal de Santa Catarina

Dedico este trabalho aos meus amados pais, pilares inabaláveis da minha vida, que sempre me ofereceram mais do que apoio, me proporcionaram a fundação sobre a qual pude construir meus sonhos. A vocês, que sacrificaram incontáveis momentos e confortos para que eu pudesse seguir adiante nos meus estudos e na minha formação. A cada página escrita, a cada desafio superado, a cada conquista celebrada, vejo o reflexo do amor, da dedicação e da crença que depositaram em mim. Esta realização não é apenas minha, mas nossa, pois foi moldada pelas vossas mãos, orientada pela vossa sabedoria e alimentada pela vossa fé inabalável em mim. Obrigado por serem meu porto seguro e minha inspiração constante.

## AGRADECIMENTOS

Gostaria de expressar minha mais profunda gratidão a todos que, de alguma forma, fizeram parte desta incrível jornada acadêmica. Aos meus professores, que não apenas compartilharam seus vastos conhecimentos técnicos, mas também me inspiraram a seguir em frente e buscar a excelência. Agradeço a todos os meus colegas de trabalho, que estiveram ao meu lado, proporcionando momentos de aprendizado colaborativo e trocas valiosas.

À minha turma e amigos mais próximos, sua ajuda emocional foi fundamental. Nos momentos mais desafiadores, foram vocês que me lembraram do motivo pelo qual comecei este projeto e me incentivaram a seguir em frente. Cada palavra de encorajamento, cada gesto de apoio, cada momento compartilhado teve um impacto profundo no meu crescimento pessoal e acadêmico.

Finalmente, a todos que direta ou indiretamente contribuíram para a conclusão deste TCC, meu sincero obrigado. Este trabalho é também um reflexo do amor, apoio e dedicação de cada um de vocês.

## RESUMO

A introdução da tecnologia blockchain na educação tem trazido benefícios significativos, como a autenticação e a disponibilidade de dados relacionados à trajetória acadêmica dos estudantes. A tokenização, em particular, oferece uma camada adicional de padronização e facilita a transferência e o compartilhamento desses dados, aumentando sua utilidade. No entanto, é importante reconhecer que mesmo sem a tokenização, os dados armazenados na blockchain podem ser bastante úteis, graças à natureza imutável e transparente da tecnologia. A tokenização é uma técnica que consiste em transformar ativos físicos ou digitais em tokens, ou seja, unidades digitais que podem ser facilmente armazenadas, transferidas e gerenciadas na blockchain. O "Jornada do Estudante" é uma plataforma que utiliza a tecnologia blockchain para armazenar os dados relacionados à trajetória acadêmica dos estudantes, como notas, histórico escolar, certificados e outras informações relevantes. O objetivo deste trabalho é implementar *badges* correspondentes a conquistas acadêmicas ao longo da vida universitária. Exemplos delas são as conquistas de melhor aluno de uma disciplina durante o semestre, melhor atleta de uma competição desportiva e de formando com melhor desempenho. Esses *badges* representam uma nova funcionalidade no projeto "Jornada do Estudante", utilizando a blockchain Hyperledger Fabric para produzir *Non-Fungible Tokens* (NFTs) no contexto educacional. Facilitando o consumo e armazenamento desses dados, bem como proporcionando uma gamificação através da emissão de *badges* educacionais e sociais, esses *badges* são representados nesse trabalho como NFTs. Foram implementados uma aplicação web onde é exibido informações educacionais e as *badges* de conquista, seguindo o padrão do "Jornada do Estudante" incluindo a implementação de um chaincode para gerenciamento das *Badges*. Desta forma, o presente trabalho contribui para o avanço da tecnologia blockchain na educação, através do desenvolvimento de uma funcionalidade para a plataforma "Jornada do Estudante" que permite emissão de *badges* educacionais e incentiva a participação dos estudantes.

**Palavras-chave:** Blockchain; Tokenização; Jornada do Estudante.

## ABSTRACT

The introduction of blockchain technology in education has brought significant benefits, such as the authentication and availability of data related to students' academic trajectories. Tokenization, in particular, offers an additional layer of standardization and facilitates the transfer and sharing of these data, enhancing their utility. However, it is important to recognize that even without tokenization, data stored on the blockchain can be quite useful, thanks to the immutable and transparent nature of the technology. Tokenization is a technique that involves transforming physical or digital assets into tokens, that is, digital units that can be easily stored, transferred, and managed on the blockchain. 'Jornada do Estudante' is a platform that uses blockchain technology to store data related to students' academic trajectories, such as grades, school history, certificates, and other relevant information. The goal of this work is to implement badges corresponding to academic achievements throughout university life. Examples include achievements for the best student in a subject during the semester, best athlete in a sports competition, and top-performing graduate. These badges represent a new feature in the 'Jornada do Estudante' project, using Hyperledger Fabric blockchain to produce Non-Fungible Tokens (NFTs) in an educational context. By facilitating the consumption and storage of these data, as well as providing gamification through the issuance of educational and social badges, these badges are represented in this work as NFTs. A web application was implemented where educational information and achievement badges are displayed, following the 'Jornada do Estudante' standard including the implementation of a chaincode for managing the Badges. Thus, this work contributes to the advancement of blockchain technology in education, through the development of a feature for the 'Jornada do Estudante' platform that allows the issuance of educational badges and encourages student participation.

**Keywords:** Blockchain; Tokenization; Jornada do Estudante.

## LISTA DE FIGURAS

Figura 1 – Lista encadeada de blocos . . . . .	15
Figura 2 – Código exemplo de um Smart Contract . . . . .	22
Figura 3 – Modelo Proposto . . . . .	36
Figura 4 – Fluxograma Front-end . . . . .	39
Figura 5 – Fluxograma Chaincode Badge . . . . .	40
Figura 6 – Página de Login . . . . .	44
Figura 7 – Página de Home . . . . .	45



## LISTA DE ABREVIATURAS E SIGLAS

API	Application Programming Interface
CSRF	Cross-Site Request Forgery
NFT	Non-Fungible Token
SDK	Software Development Kit
TCC	Trabalho de conclusão de curso
TLD	Tecnologia de ledger distribuído
TPS	Transações por segundo

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b> . . . . .	<b>12</b>
1.1	OBJETIVOS . . . . .	13
1.1.1	<b>Objetivo Geral</b> . . . . .	<b>13</b>
1.1.2	<b>Objetivos Específicos</b> . . . . .	<b>13</b>
1.2	METODOLOGIA . . . . .	13
1.3	ESTRUTURA DO DOCUMENTO . . . . .	14
<b>2</b>	<b>FUNDAMENTAÇÃO TEÓRICA</b> . . . . .	<b>15</b>
2.1	BLOCKCHAIN . . . . .	15
2.1.1	<b>PRINCÍPIOS E APLICAÇÕES DA TECNOLOGIA BLOCK-CHAIN</b> . . . . .	<b>16</b>
2.1.2	<b>TIPOS DE REDE BLOCKCHAIN</b> . . . . .	<b>16</b>
2.1.2.1	<i>Blockchain Pública</i> . . . . .	16
2.1.2.2	<i>Blockchain Privada</i> . . . . .	16
2.1.2.3	<i>Blockchain de Consórcio</i> . . . . .	16
2.1.2.4	<i>Algoritmos de consenso</i> . . . . .	17
2.2	HYPERLEDGER FABRIC . . . . .	17
2.2.1	<b>BLOCKCHAIN DE CONSÓRCIO E CARACTERÍSTICAS DE CONCEÇÃO</b> . . . . .	<b>18</b>
2.2.2	<b>PRINCIPAIS CARACTERÍSTICAS DO HYPERLEDGER FABRIC</b> . . . . .	<b>19</b>
2.2.3	<b>TRANSAÇÕES EM HYPERLEDGER FABRIC</b> . . . . .	<b>19</b>
2.2.3.1	<i>Iniciando uma Transação</i> . . . . .	19
2.2.3.2	<i>Verificação e Execução da Transação pelos Nós de Endosso</i> . . . . .	19
2.2.3.3	<i>Inspeção das Respostas da Proposta</i> . . . . .	19
2.2.3.4	<i>Reunião dos Endossos em uma Transação</i> . . . . .	20
2.2.3.5	<i>Validação e Confirmação da Transação</i> . . . . .	20
2.2.3.6	<i>Atualização do Livro-Razão</i> . . . . .	20
2.3	FERRAMENTAS DE DESENVOLVIMENTO . . . . .	20
2.4	ETHEREUM E SMART CONTRACTS . . . . .	21
2.4.1	<b>FUNDAMENTAÇÃO TÉORICA</b> . . . . .	<b>21</b>
2.4.1.1	<i>Origem e desenvolvimento do Ethereum</i> . . . . .	21
2.4.1.2	<i>Princípios fundamentais do Ethereum</i> . . . . .	21
2.4.2	<b>SMART CONTRACTS</b> . . . . .	<b>21</b>
2.5	NON-FUNGIBLE TOKEN (NFT) . . . . .	23
2.5.1	<b>OPORTUNIDADES DOS NFTs</b> . . . . .	<b>23</b>
2.5.2	<b>DESAFIOS DOS NFTs</b> . . . . .	<b>23</b>
2.5.2.1	<i>Desafios de Usabilidade</i> . . . . .	24

2.5.2.2	<i>Questões de Segurança e Privacidade</i> . . . . .	24
2.5.2.3	<i>Questões de Governança</i> . . . . .	25
2.5.2.4	<i>Questões de Extensibilidade</i> . . . . .	26
<b>3</b>	<b>TRABALHOS CORRELATOS</b> . . . . .	<b>28</b>
3.1	A NEW DECENTRALIZED CERTIFICATION VERIFICATION PRIVACY CONTROL PROTOCOL . . . . .	28
3.2	EDUCATIONAL APPLICATIONS OF NON-FUNGIBLE TOKEN (NFT) . . . . .	29
3.3	DEVELOPMENT OF A BLOCKCHAIN-BASED APPLICATION FOR DIGITAL CERTIFICATES IN EDUCATION . . . . .	30
3.4	NON-FUNGIBLE TOKENS, DECENTRALIZED AUTONOMOUS ORGANIZATIONS, WEB 3.0, AND THE METAVERSE IN EDUCATION: FROM UNIVERSITY TO METAVERSITY . . . . .	30
3.5	FABASSET: UNIQUE DIGITAL ASSET MANAGEMENT SYSTEM FOR HYPERLEDGER FABRIC . . . . .	30
<b>4</b>	<b>PROPOSTA</b> . . . . .	<b>32</b>
4.1	INTRODUÇÃO . . . . .	32
4.2	GAMIFICAÇÕES A SEREM IMPLEMENTADAS . . . . .	32
<b>4.2.1</b>	<b>Melhor Atleta de um Campeonato</b> . . . . .	<b>33</b>
<b>4.2.2</b>	<b>Melhor Aluno da Disciplina no Semestre</b> . . . . .	<b>33</b>
<b>4.2.3</b>	<b>Melhor Aluno do Curso na Formatura</b> . . . . .	<b>33</b>
4.3	PRIVACIDADE DAS BADGES . . . . .	33
4.4	TRANSPORTE DE BADGES PARA BLOCKCHAINS PÚBLICAS . . . . .	34
4.5	WORKFLOW DE GERAÇÃO DAS BADGES . . . . .	34
4.6	IMPLEMENTAÇÃO . . . . .	35
4.7	CONTRIBUIÇÕES DA PROPOSTA . . . . .	36
<b>5</b>	<b>PROTOTIPO</b> . . . . .	<b>38</b>
5.1	INTRODUÇÃO . . . . .	38
5.2	CHAINCODE . . . . .	39
5.2.0.1	<i>Estrutura do Chaincode</i> . . . . .	39
5.2.0.2	<i>Funções Principais do Chaincode</i> . . . . .	40
5.2.0.3	<i>Implementação e Lógica de Negócios</i> . . . . .	41
5.2.0.4	<i>Considerações de Segurança e Melhores Práticas</i> . . . . .	41
5.3	FRONT-END . . . . .	42
<b>5.3.1</b>	<b>Organização do código</b> . . . . .	<b>42</b>
<b>5.3.2</b>	<b>Arquivos da Raiz do Projeto</b> . . . . .	<b>43</b>
5.3.2.1	<i>Arquivo main.tsx</i> . . . . .	43
5.3.2.2	<i>Arquivo app.tsx</i> . . . . .	43
5.3.2.3	<i>Arquivo Router.tsx</i> . . . . .	43

5.3.3	<b>Páginas da Aplicação</b> . . . . .	43
5.3.3.1	<i>Página de Login</i> . . . . .	43
5.3.3.2	<i>Página de Home</i> . . . . .	44
5.4	<b>INTEGRAÇÃO COM A BLOCKCHAIN JORNADA DO ESTUDANTE</b>	46
5.4.1	<b>Configuração do Ambiente de Desenvolvimento</b> . . . . .	46
5.4.2	<b>Construção e Execução da Rede Blockchain</b> . . . . .	46
5.4.3	<b>Instalação e Inicialização dos Chaincodes</b> . . . . .	46
5.4.4	<b>Inicialização dos Aplicativos</b> . . . . .	46
5.4.5	<b>Inicialização da API</b> . . . . .	47
5.5	<b>DESAFIOS</b> . . . . .	47
5.5.1	<b>Compreensão e Implementação da Hyperledger Fabric</b> . . . . .	47
5.5.2	<b>Autenticação com o GovBr</b> . . . . .	47
5.5.3	<b>Gerenciamento de Permissões no Chaincode</b> . . . . .	47
5.5.4	<b>Comunicação entre API e Aplicativo</b> . . . . .	48
5.5.5	<b>Integração com Blockchain Pública</b> . . . . .	48
6	<b>CONCLUSÃO</b> . . . . .	49
	<b>REFERÊNCIAS</b> . . . . .	50
	<b>APÊNDICE A – Artigo da monografia</b> . . . . .	54

## 1 INTRODUÇÃO

No dia 31 de outubro de 2008, uma figura, anônima até então, alteraria definitivamente o curso da história da computação distribuída. No *whitepaper* "Bitcoin: A Peer-to-peer Electronic Cash System"(NAKAMOTO, 2008), Satoshi Nakamoto estabeleceu os alicerces do que se conhece hoje como criptomoeda e blockchain. O autor anônimo criou uma criptomoeda conhecida como Bitcoin, uma moeda digital representado uma cadeia de assinaturas digitais e evidências criptográficas transmitidos a outros por meio de uma rede *peer-to-peer* descentralizada.

A rede blockchain tem potencial significativo para transformar a prestação de serviços governamentais, simplificando a troca de informações e coordenando processos entre diversas agências governamentais. Por exemplo, países como a Suécia estão explorando essa tecnologia para agilizar seus registros de propriedades, diminuindo o risco de fraudes e tornando as transferências mais eficientes (REGISTRY, 2018). Além disso, a Estônia tem utilizado a blockchain para estabelecer sistemas de identidade digital, permitindo uma validação de identidade online rápida e segura (E-ESTONIA, 2018).

Desta forma, o Ministério da Educação (MEC) viu o uso de blockchain como oportunidade de aperfeiçoar a rede de ensino, deixando-a segura e rápida. Considerando problemas no sistema de instituições de ensino, os autores (PALMA *et al.*, 2019) propuseram uma novo modelo de blockchain e *smart contracts* nas instituições de ensino superior, onde seria possível guardar dados do processo de formação de maneira transparente e segura. O MEC apreciou esta proposta e iniciou o projeto com o Laboratório de Segurança em Computação (LABSEC) da Universidade Federal de Santa Catarina (UFSC). Entretanto, esse modelo não abrange a parte de *tokenization* na rede, a qual transformaria os *badges* dos usuários da Jornada do Estudante em *Token*.

Este vigente trabalho tem como finalidade realizar a criação de estruturas para permitir a emissão desses *badges*, que é apresentado ou exibido para indicar alguma realização, além da estrutura, o presente trabalho busca criar um processo de gamificação para o estudante, visando criar um módulo desta solução dentro do "Jornada do Estudante"(MEC, s.d.). Isso possibilitará que todas as conquistas acadêmicas e extra-curriculares sejam tokenizáveis e lastreáveis na rede, ampliando o seu uso.

## 1.1 OBJETIVOS

### 1.1.1 Objetivo Geral

Desenvolver uma estrutura a possibilitar a emissão de *badges* para o Jornada do Estudante, de forma a facilitar o consumo e armazenamento dos dados relacionados à graduação e demais etapas de ensino, representando esses *badges* de forma integrativa ao usuário, trazendo o fornecimento de uma gameficação ao aplicativo e à rede, gerando uma maior utilização do mesmo.

### 1.1.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

1. Criar os artefatos de software necessários para a emissão de *badges* na blockchain.
2. Possibilitar uma gamificação, através da qual o usuário da rede consiga visualizar e localizar suas *badges* na blockchain.
3. Testar a estrutura, criando *badges* na blockchain.

## 1.2 METODOLOGIA

Em uma primeira etapa, foi utilizado o método de leituras exploratórias com foco nas tecnologias utilizadas no projeto. Esta etapa consistiu em realizar um estudo para entender os conceitos de blockchain e tokenização e seu funcionamento, além de realizar uma fundamentação teórica para a plataforma Hyperledger Fabric (IBM, 2022), que possui características específicas em relação ao seu funcionamento numa rede blockchain.

O principal objetivo desta etapa é abranger o conhecimento sobre a tokenização e gamificação de usuários numa rede blockchain e sobre protocolos de comunicação web para então definir a melhor maneira de realizar os objetivos do projeto. Em sequência, antes de iniciar o desenvolvimento do protótipo foram localizados projetos com temas semelhantes ao proposto neste trabalho para identificar o estado da arte atual.

Aplicações de cunho acadêmico relacionadas ao tema deste trabalho foram utilizadas como uma base estrutural para o desenvolvimento do protótipo. O objetivo desta etapa é identificar o que há de mais novo no mercado e utilizar disso para deixar o resultado o mais agradável possível para o usuário final. Caso tecnologias novas sejam descobertas, foi realizada uma etapa de estudos focada no entendimento e na absorção de conhecimentos relacionados às novas ferramentas, logo após, buscou-se entender conceitos de usabilidade e como aplicá-lá no protótipo a ser desenvolvido, pois o trabalho em questão é voltado para um usuário comum e não alguém com conhecimentos técnicos.

### 1.3 ESTRUTURA DO DOCUMENTO

Este Trabalho de conclusão de curso (TCC) inicia com a Introdução no Capítulo 1, que apresenta uma visão geral do estudo, incluindo os objetivos e a metodologia utilizada. Em seguida, no Capítulo 2 é fornecida uma fundamentação teórica dos principais conceitos envolvidos neste trabalho, abordando blockchain, Hyperledger Fabric, Ethereum e Non-Fungible Token (NFT). No Capítulo 3, são revisados trabalhos relacionados ao tema do TCC, fornecendo uma visão geral do estado atual da arte. O Capítulo 4 apresenta a proposta do trabalho, discutindo a solução proposta para o problema identificado. Já no Capítulo 5, é descrito em detalhes o desenvolvimento do protótipo, incluindo a estrutura do chaincode, a organização do código front-end, e a integração com a blockchain Jornada do Estudante. Ele também aborda os desafios enfrentados durante o desenvolvimento e as soluções adotadas. O último Capítulo, de número 6, resume as principais descobertas e contribuições do trabalho, além de sugerir direções para pesquisas futuras. Este capítulo reflete sobre o impacto do projeto no campo da educação e da tecnologia blockchain.

## 2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo introduz ao leitor os conceitos necessários para entender como funcionam as tecnologias relacionadas a este trabalho e os motivos de serem utilizadas.

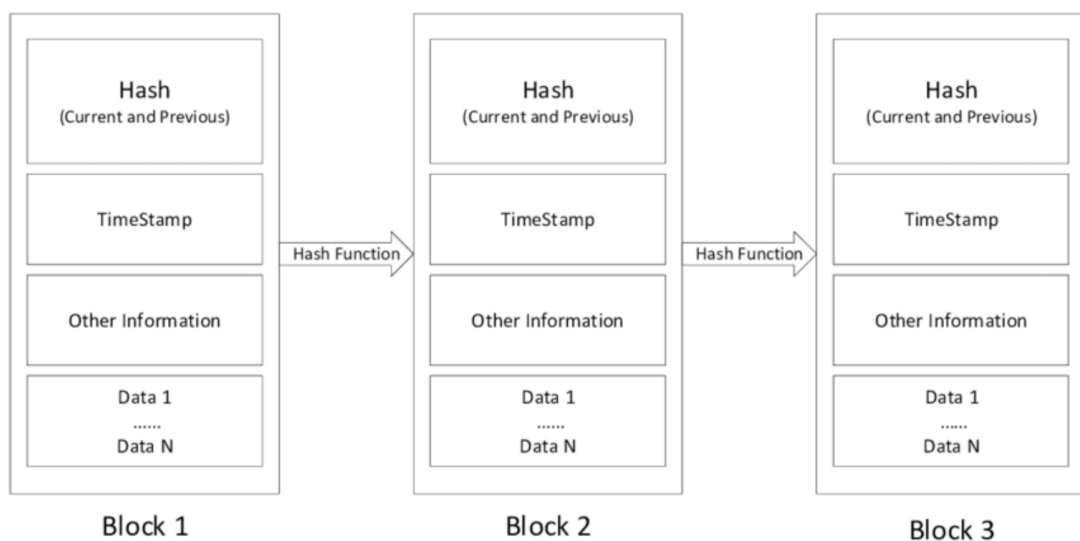
### 2.1 BLOCKCHAIN

A Blockchain é uma tecnologia disruptiva para a construção de consenso e confiança em uma rede *peer-to-peer* sem controle centralizado. Foi usada pela primeira vez no Bitcoin, a primeira criptomoeda lançada no início de 2009, para implementar um livro razão seguro de transações. A imutabilidade do livro razão (*ledger*), que corresponde a uma lista encadeada de blocos (ver Figura 1), é uma característica fundamental para assegurar a integridade das transações em uma moeda digital. Ela garante que, após uma transação ser registrada, não possa ser facilmente alterada.

No entanto, essa imutabilidade por si só não resolve o desafio do gasto duplo. O gasto duplo refere-se à tentativa de usar a mesma moeda digital em mais de uma transação. Para combater isso, criptomoedas como o Bitcoin empregam mecanismos de consenso, como a prova de trabalho (Proof of Work - PoW). Esse mecanismo valida e confirma transações, tornando extremamente desafiador gastar a mesma moeda duas vezes. Portanto, enquanto a imutabilidade protege a integridade das transações, é o mecanismo de consenso que previne efetivamente o gasto duplo. (ZHAO *et al.*, 2021).

Após um período de tranquilidade, o interesse pela blockchain explodiu nos últimos anos. O número de publicações indexadas pela *Web of Science* sobre blockchain aumentou de 2 em 2013 (o primeiro ano em que publicações sobre blockchain começaram a aparecer), para 4 em 2014, 21 em 2015, 118 em 2016, 521 em 2017 e 1.080 em 2018 (ZHAO *et al.*,

Figura 1 – Lista encadeada de blocos



Fonte: (ARCHANA PRASHANTH JOSHI MENG HAN, 2018)



2021).

### 2.1.1 PRINCÍPIOS E APLICAÇÕES DA TECNOLOGIA BLOCKCHAIN

As atividades de pesquisa e desenvolvimento relacionadas à tecnologia blockchain podem ser divididas em duas áreas: (1) A aplicação do blockchain em vários setores da indústria, como fintech, medicina e saúde, energia e sistemas de geração de energia, imóveis, viagens, manufatura, educação ou até mesmo governo (SETORES, 2021); (2) Pesquisa fundamental sobre a própria tecnologia blockchain, como algoritmos de consenso alternativos que consomem menos energia, proporcionam melhor escalabilidade, são mais robustos contra ataques cibernéticos e são mais escaláveis.

No primeiro caso, questões interessantes podem surgir devido às necessidades específicas de uma aplicação. Por exemplo, a blockchain pode ser usado para garantir a segurança dos dados produzidos por uma rede de sensores. No entanto, a quantidade de dados pode facilmente exceder a capacidade de qualquer plataforma de blockchain atual. Para a segunda área, vimos algoritmos de consenso alternativos sendo propostos, como prova de participação, que provavelmente tornarão as blockchains mais escaláveis, seguros e robustos a longo prazo.

### 2.1.2 TIPOS DE REDE BLOCKCHAIN

#### 2.1.2.1 *Blockchain Pública*

Estas redes permitem que qualquer pessoa participe da rede e execute transações visíveis a todos os usuários da rede. Não há relação de confiança entre os usuários da rede antes de se juntar à rede. A transação pode ser verificada por qualquer nó. Todos os nós participam do processo de consenso da transação. (SIAL, 2019).

#### 2.1.2.2 *Blockchain Privada*

Refere-se a uma blockchain onde o acesso aos dados é limitado a um grupo específico. No entanto, isso não necessariamente implica que todos os membros desse grupo possam validar transações ou participar do processo de consenso. Uma instância privada do Ethereum, que é a blockchain que permite a criação de apps e a transferência de ativos digitais por exemplo, pode ser acessada apenas por membros de uma organização específica, mas nem todos os membros podem necessariamente criar ou validar transações. (SIAL, 2019).

#### 2.1.2.3 *Blockchain de Consórcio*

Esta rede é uma forma colaborativa de rede blockchain, onde os participantes são entidades conhecidas, como organizações ou empresas, ao invés de indivíduos anônimos

encontrados em blockchains públicas. Estas entidades se unem para criar e operar uma blockchain compartilhada, trabalhando juntas para alcançar objetivos comuns. Diferente das blockchains públicas, onde qualquer pessoa pode participar, e das blockchains privadas, gerenciadas por uma única organização, os consórcios são coletivamente gerenciados por seus membros. Isso permite que as organizações aproveitem os benefícios da tecnologia blockchain, como transparência e imutabilidade, em um ambiente controlado e colaborativo. Comumente, esses consórcios são formados para abordar desafios específicos de um setor ou para desenvolver soluções inovadoras que beneficiem todos os membros. (SIAL, 2019).

#### 2.1.2.4 Algoritmos de consenso

O algoritmo de consenso é um componente fundamental das redes blockchain e sistemas distribuídos. Ele serve para garantir que todos os participantes de uma rede cheguem a um acordo comum sobre o estado atual da rede, mesmo na presença de nós mal-intencionados ou falhas no sistema. Em uma blockchain, as transações são agrupadas em blocos, e esses blocos são adicionados à cadeia de forma sequencial. No entanto, em uma rede descentralizada, diferentes participantes podem criar blocos simultaneamente ou ter visões diferentes sobre qual bloco deve ser o próximo na sequência. O algoritmo de consenso é o mecanismo que resolve essas discrepâncias, garantindo que todos os participantes concordem sobre a ordem dos blocos e o conteúdo da blockchain.

- Proof of Work (PoW): O PoW requer que os mineradores, que funciona como um processo para validar e incluir novas transações no blockchain, solucionem desafios matemáticos para adicionar um novo bloco à cadeia. O minerador que primeiro decifra esse desafio tem o privilégio de adicionar o próximo bloco, que é posteriormente verificado pelos demais participantes. Embora seja uma abordagem segura, é notoriamente conhecida por seu alto consumo energético (LIN, 2023).
- Proof of Stake (PoS): Diferentemente do PoW, que se baseia em capacidade computacional, o PoS seleciona os participantes para adicionar o próximo bloco com base em sua participação na moeda. Isso significa que quanto mais moeda um participante detiver e estiver disposto a colocar como "garantia", maior será sua chance de criar um bloco. Esta metodologia é vista como uma alternativa mais sustentável ao PoW, devido à sua eficiência energética superior (LIN, 2023).

## 2.2 HYPERLEDGER FABRIC

O Hyperledger Fabric é uma plataforma de Tecnologia de ledger distribuído (TLD) de nível empresarial, autorizada, e um produto de destaque no panorama da tecnologia de cadeias de blocos. Foi concebida para suportar implementações de diferentes componentes

e acomodar as complexidades existentes no ecossistema económico. É sustentada por uma arquitetura modular que proporciona elevados graus de confidencialidade, resiliência, flexibilidade e escalabilidade. Esta plataforma é conhecida pela sua utilização em contextos empresariais (NOTÍCIA, s.d.) isso incluindo bancos, finanças, seguros, assistência médica, recursos humanos, cadeia de suprimentos e até distribuição de música digital e oferece capacidades diferenciadoras essenciais em relação a outras plataformas populares de livro-razão distribuído ou de cadeias de blocos.

A Hyperledger Foundation, um esforço de colaboração de código aberto criado para fazer avançar as tecnologias de cadeia de blocos entre sectores, é a força motriz por detrás do Hyperledger Fabric. Acolhida pela Linux Foundation, reúne líderes em domínios como as finanças, a banca, a Internet das Coisas, a cadeia de abastecimento, o fabrico e a tecnologia. A Hyperledger Foundation acolhe uma série de projectos de software de cadeia de blocos de nível empresarial, sendo o Hyperledger Fabric um dos mais proeminentes. Estes projectos são concebidos e construídos por uma comunidade de programadores diversificada e servem uma vasta gama de partes interessadas, incluindo fornecedores, organizações de utilizadores finais, prestadores de serviços, empresas em fase de arranque, académicos e muito mais. O objetivo é fornecer as ferramentas necessárias para construir e implementar redes de cadeias de blocos ou soluções comerciais. Os colaboradores da Hyperledger Foundation, como parte da equipe mais vasta da Linux Foundation, possui anos de experiência na prestação de serviços de gestão de programas para projectos de código aberto (HYPERLEDGER, 2023).

### **2.2.1 BLOCKCHAIN DE CONSÓRCIO E CARACTERÍSTICAS DE CONCEÇÃO**

O Hyperledger Fabric é um exemplo proeminente de cadeias de blocos de consórcio, que se caracterizam pela autenticação de blocos efectuada por um conjunto específico de nós. É uma blockchain semi-privada a leitura das informações pode ser pública, ou seja, qualquer pessoa pode visualizar as transações e os dados armazenados. No entanto, a permissão para escrever ou validar transações é restrita a um grupo específico de participantes. Isso significa que, embora o público em geral possa ter acesso para ver as transações, apenas entidades autorizadas podem criar e validar novas transações, representando um sistema parcialmente centralizado controlado por alguns nós seletores. Esta conceção permite que os nós da rede com autoridade configurem os dados na cadeia de blocos para serem públicos ou privados.

Concebido para criar um consórcio, ou um grupo de redes, o Hyperledger Fabric permite que um grupo de empresas estabeleça uma rede, em que cada participante possui um ou mais nós. Esta estrutura suporta transações privadas e confidenciais que são imutáveis, verificáveis e eficientes em termos de desempenho. Além disso, permite que os consórcios tomem decisões de adesão, proporcionando assim uma arquitetura modular que

a distingue de outras soluções de cadeia de blocos (HYPERLEDGER, 2023).

### 2.2.2 PRINCIPAIS CARACTERÍSTICAS DO HYPERLEDGER FABRIC

As características definidoras do Hyperledger Fabric incluem uma arquitetura altamente modular e configurável, que permite versatilidade e otimização numa vasta gama de casos de utilização da indústria. Esta conceção permite a sua adaptação às necessidades específicas de vários setores, desde finanças aos cuidados de saúde, entre outros. Além disso, como uma cadeia de blocos autorizada, garante que os registos digitais podem ser encriptados e são visíveis apenas para participantes autorizados, cumprindo os requisitos de privacidade necessários em aplicações empresariais (HYPERLEDGER, 2023).

### 2.2.3 TRANSAÇÕES EM HYPERLEDGER FABRIC

O fluxo de transações no Hyperledger Fabric destaca a robustez e a segurança da plataforma. Cada etapa do processo é projetada para garantir a integridade e a autenticidade das transações, tornando o Hyperledger Fabric uma escolha ideal para aplicações que exigem transações seguras e confiáveis. O fluxo de transações é composto por seis etapas: proposta, endosso, verificação, consenso, validação e compromisso.

#### 2.2.3.1 *Iniciando uma Transação*

O fluxo de transações começa quando um cliente inicia uma solicitação para executar uma transação. Esta solicitação é enviada para os nós de endosso, que são responsáveis por executar a transação e endossar os resultados.

#### 2.2.3.2 *Verificação e Execução da Transação pelos Nós de Endosso*

Os nós de endosso recebem a proposta de transação e verificam se ela está corretamente formada, se não foi enviada anteriormente (para proteger contra ataques de repetição), se a assinatura é válida e se o remetente está autorizado a executar a transação proposta. Após a verificação, o chaincode é executado no banco de dados do estado atual para produzir os resultados da transação.

#### 2.2.3.3 *Inspeção das Respostas da Proposta*

O aplicativo cliente verifica as assinaturas dos nós de endosso e compara as respostas da proposta. Se a política de endosso foi cumprida, a transação é enviada ao serviço de ordenação.

#### 2.2.3.4 Reunião dos Endossos em uma Transação

O aplicativo cliente reúne os endossos em uma transação e a transmite para o serviço de ordenação. A transação contém os conjuntos de leitura/gravação, as assinaturas dos nós de endosso e o ID do canal.

#### 2.2.3.5 Validação e Confirmação da Transação

Os blocos de transações são entregues a todos os nós no canal. As transações dentro do bloco são validadas para garantir que a política de endosso foi cumprida e que não houve alterações no estado do livro-razão desde que o conjunto de leitura foi gerado. As transações são então marcadas como válidas ou inválidas.

#### 2.2.3.6 Atualização do Livro-Razão

Para cada transação válida, os conjuntos de gravação são confirmados no banco de dados do estado atual. Cada nó anexa o bloco à cadeia do canal e emite um evento para notificar o aplicativo cliente de que a transação foi anexada à cadeia de registros imutáveis e que a transação foi validada ou invalidada.

### 2.3 FERRAMENTAS DE DESENVOLVIMENTO

As ferramentas de desenvolvimento desempenham um papel crucial na criação e implementação de soluções baseadas em blockchain. No contexto do Hyperledger Fabric, existem várias ferramentas e linguagens que são comumente usadas.

**Linguagens de Chaincode:** O Chaincode é o termo usado pelo Hyperledger Fabric para se referir aos contratos inteligentes que são executados na blockchain. As linguagens de programação suportadas para escrever chaincodes incluem Go, JavaScript e TypeScript. Cada uma dessas linguagens tem suas próprias vantagens e desvantagens, e a escolha da linguagem de programação pode depender de vários fatores, como a complexidade do contrato inteligente, as habilidades da equipe de desenvolvimento e as necessidades específicas do projeto.

**SDKs/Gateways:** As Software Development Kits (SDKs) e os gateways fornecem uma interface para interagir com a rede blockchain. Eles permitem que os desenvolvedores criem e gerenciem transações, interajam com contratos inteligentes e realizem outras tarefas relacionadas à blockchain. O Hyperledger Fabric suporta SDKs para várias linguagens de programação, incluindo Node.js, Java e Go.

**Hyperledger Caliper:** O Hyperledger Caliper é uma ferramenta de benchmarking que permite aos usuários medir o desempenho de uma blockchain específica sob várias cargas de trabalho. Caliper suporta várias plataformas blockchain, incluindo Hyperledger Fabric, e pode ser uma ferramenta valiosa para testar e otimizar o desempenho de uma solução blockchain.

Essas ferramentas e linguagens de programação formam a base para o desenvolvimento de aplicações robustas e eficientes na blockchain Hyperledger Fabric. A escolha das ferramentas certas pode ter um impacto significativo na qualidade e eficácia da solução final.

## 2.4 ETHEREUM E SMART CONTRACTS

Ethereum é uma plataforma de software baseada em blockchain que permite a construção e execução de contratos inteligentes e as chamadas Aplicações Distribuídas (DApps). Essa plataforma também é a base para uma moeda virtual relacionada, chamada Ether. Para a definição de contratos inteligentes, o Ethereum fornece uma linguagem de programação Turing completa que permite criar programas e executá-los no blockchain (FERRETTI; D'ANGELO, 2019).

### 2.4.1 FUNDAMENTAÇÃO TÉORICA

#### 2.4.1.1 *Origem e desenvolvimento do Ethereum*

O Ethereum foi proposto pela primeira vez em 2013 por Vitalik Buterin, um programador envolvido com o Bitcoin. Buterin acreditava que o Bitcoin precisava de uma linguagem de script para o desenvolvimento de aplicativos. Quando a proposta não foi aceita, ele sugeriu o desenvolvimento de uma nova plataforma com uma linguagem de script mais geral (FERRETTI; D'ANGELO, 2019).

#### 2.4.1.2 *Princípios fundamentais do Ethereum*

O Ethereum opera usando contas e seus saldos, que mudam por meio de transições de estado. O estado denota os saldos atuais de todas as contas, além de outros possíveis dados extras. O estado não é armazenado no blockchain diretamente, mas é codificado e mantido por contas em uma estrutura de dados separada organizada como uma árvore Patricia Merkle (FERRETTI; D'ANGELO, 2019).

### 2.4.2 SMART CONTRACTS

Os smart contracts, ou contratos inteligentes, são scripts que estão ancorados em uma blockchain ou infraestrutura distribuída semelhante. Quando acionados por uma transação na blockchain e validados em toda a rede, ações predefinidas são executadas. Dado que as condições de um smart contract são armazenadas de forma transparente na blockchain, ele sempre operará conforme todas as partes pretendem, o que pode reduzir questões de confiança entre as partes envolvidas. Esses contratos são, em essência, scripts de software, semelhantes aos scripts que são executados em aplicações que não são baseadas em blockchain.

O conceito e a ideia subjacente dos smart contracts precedem a emergência do Bitcoin e da tecnologia blockchain. (SZABO, 1994) definiu um smart contract como um protocolo de transação informatizado que atende a condições contratuais, como termos de pagamento, confidencialidade ou execução, reduzindo exceções e minimizando a necessidade de intermediários confiáveis. Ele citou protocolos de dinheiro digital como exemplos de smart contracts, pois esses mecanismos permitem pagamentos online combinados com características de dinheiro em papel, como divisibilidade e confidencialidade.

No entanto, é importante notar que tanto o termo "smart" quanto "contract" podem ser enganosos. Um smart contract consiste em um código de computador simples e raramente representa um constructo legalmente vinculativo. Buterin, o fundador da Ethereum, expressou arrependimento por adotar o termo "smart contracts", sugerindo que deveria ter escolhido um nome mais técnico e menos sugestivo (TOLE SUTIKNO, 2021).

Um exemplo simples de um smart contract é um sistema automatizado de gerenciamento de quartos de hotel. Assim que um cliente deixa o quarto, o smart contract é automaticamente notificado. Por exemplo, um dispositivo conectado à porta do quarto atua como um oráculo que inicia transações na blockchain sempre que a porta é usada. Isso, por sua vez, aciona processos predefinidos, como faturamento ou atribuição automática de pessoal de limpeza.

No caso da Ethereum, os smart contracts são escritos em uma linguagem de programação Turing completa chamada Solidity. A linguagem é compilada em bytecode e executada na máquina virtual Ethereum (EVM). Transações assinadas por chaves privadas podem invocar a execução de funções de um smart contract. Pode-se ver um exemplo de smart contract em Solidity na Figura 2, o qual possui uma função que retorna o saldo do contrato em Eth, criptomoeda da Ethereum.

Figura 2 – Código exemplo de um Smart Contract

```
1 // Codigo exemplo de um Smart Contract
2
3 pragma solidity ^0.8.0;
4
5 contract Balance {
6     function balance() public returns (uint256){
7         return payable(address(this)).balance;
8     }
9 }
```

A tecnologia blockchain, que permite a transferência segura de valor peer-to-peer (p2p) pela internet entre partes que não confiam mutuamente, ofereceu pela primeira vez uma infraestrutura distribuída adequada para a aplicação de smart contracts. Uma vez que os termos predefinidos são cumpridos, a blockchain executa transparentemente o código, e nenhuma entidade externa pode interferir (TOLE SUTIKNO, 2021).

## 2.5 NON-FUNGIBLE TOKEN (NFT)

Os NFT são um tipo de criptomoeda que é derivada dos contratos inteligentes do Ethereum. O NFT foi proposto pela primeira vez nas Propostas de Melhoria do Ethereum (EIP)-721 e posteriormente desenvolvido no EIP-1155(WANG *et al.*, 2021). Os NFTs diferem das criptomoedas clássicas, como o Bitcoin, em suas características intrínsecas. O Bitcoin é uma moeda padrão na qual todas as moedas são equivalentes e indistinguíveis. Em contraste, o NFTs é único e não pode ser trocado como se fosse igual (ou seja, não fungível), tornando-o adequado para identificar algo ou alguém de maneira única (WANG *et al.*, 2021).

Os NFTs têm atraído notável atenção tanto da comunidade industrial quanto científica. Foi relatado que o volume médio de negociação de 24 horas do mercado de NFTs é de 4,592,146,914 USD, enquanto o volume de negociação de 24 horas de todo o mercado de criptomoedas é de 341,017,001,809 USD (WANG *et al.*, 2021). A liquidez das soluções relacionadas ao NFT representou 1,3% de todo o mercado de criptomoedas em um curto período (5 meses)(WANG *et al.*, 2021).

### 2.5.1 OPORTUNIDADES DOS NFTs

Os NFTs têm grande potencial na indústria de jogos. Já existem alguns jogos cripto como CryptoKitties, Cryptocats, CryptoPunks, Meebits, Axie Infinity, Gods Unchanged, e TradeStars. Uma característica fascinante desses jogos é o mecanismo de "criação". Os usuários podem criar pessoalmente animais de estimação e passar muito tempo criando novos descendentes. Os NFTs também promovem o desenvolvimento da arte, eventos de bilheteria, valor, IoT e finanças. Outros tipos de mercados circundantes desempenham papéis importantes também para fornecer informações instantâneas e ambientes seguros, como sites de estatísticas (por exemplo, NonFungible, DappRadar, NFT bank, DeFiPulse, Coingecko), mercado de negociação (cryptoslam, Opensea, SuperRare, Nifty Gateway, Rarible, Zora) e o chamado ecossistema NFT (como DeGo)(WANG *et al.*, 2021).

### 2.5.2 DESAFIOS DOS NFTs

Para permitir o desenvolvimento das aplicações de NFT acima, uma série de barreiras precisa ser superada, como acontece com qualquer tecnologia nascente. Discutimos alguns desafios típicos das perspectivas de usabilidade, segurança, governança e extensibilidade, cobrindo tanto os problemas de nível de sistema causados pelas plataformas baseadas em blockchain quanto os fatores humanos, como governança, regulamentação e sociedade.



### 2.5.2.1 Desafios de Usabilidade

A usabilidade é uma medida da eficácia, eficiência e satisfação dos usuários ao testar um produto ou design específico. A maioria dos esquemas de NFT é construída com base no Ethereum. Portanto, as principais desvantagens do Ethereum ainda existem. Discutimos dois desafios principais que têm impactos diretos na experiência do usuário (WANG *et al.*, 2021):

- **Confirmação Lenta:** Os procedimentos relacionados ao NFT são normalmente conduzidos enviando transações por meio do contrato inteligente para uma gestão confiável e transparente (como cunhagem, venda, troca). No entanto, os sistemas atuais de NFT estão intimamente acoplados com suas plataformas de blockchain subjacentes, o que os faz sofrer de baixo desempenho (Bitcoin atinge apenas 7 Transações por segundo (TPS) enquanto Ethereum apenas 30 TPS). Isso resulta em uma confirmação extremamente lenta dos NFTs. Conquistar esse problema requer uma reformulação dos sistemas de blockchain, otimização de sua estrutura ou melhoria nos mecanismos de consenso. Os sistemas de blockchain existentes não podem cumprir tais requisitos (WANG *et al.*, 2021).
- **Altos Preços de Gas:** Os altos preços do gas se tornaram um grande problema para os mercados de NFT, especialmente ao cunhar os NFTs em grande escala, o que requer o upload dos metadados para a rede blockchain. Todas as transações relacionadas ao NFT são mais caras do que uma simples transação de transferência porque os contratos inteligentes envolvem recursos computacionais e armazenamento para serem processados. No momento da escrita, para minerar um token NFT custa mais de 60 USD (equivalente a cerca de  $5 \times 10^2$ wei) 1. Para completar uma simples negociação de NFT pode custar entre 60 e 100 USD para cada transação. As taxas caras causadas por operações complexas e alta congestão limitam muito sua ampla adoção (WANG *et al.*, 2021).

### 2.5.2.2 Questões de Segurança e Privacidade

A segurança dos dados do usuário é a primeira prioridade dos sistemas. No entanto, os dados (armazenados fora da cadeia, mas relacionados às tags na cadeia) enfrentam o risco de perder a ligação ou serem mal utilizados por partes mal-intencionadas. Damos detalhes a seguir (WANG *et al.*, 2021):

- **Inacessibilidade de Dados NFT:** Nos principais projetos NFT, um "hash" criptográfico como o identificador, em vez de uma cópia do arquivo, será marcado com o token e então registrado no blockchain para economizar o consumo de gas. Isso faz com que o usuário perca a confiança no NFT porque o arquivo original pode ser perdido ou danificado. Vários projetos NFT integram seu sistema com um sistema de armazenamento de arquivos especializado, como o IPFS, no qual os

endereços IPFS permitem que os usuários encontrem um pedaço de conteúdo, desde que alguém em algum lugar na rede IPFS esteja hospendo. No entanto, esses sistemas têm falhas. Quando os usuários "enviam" metadados NFT para os nós IPFS, não há garantia de que seus dados serão replicados entre todos os nós. Os dados podem se tornar inacessíveis se o ativo for armazenado no IPFS e o único nó que o armazena for desconectado da rede. Este problema foi relatado por DECRYPT.IO e CHECKMYNFT.COM . Além disso, um NFT pode apontar para um endereço de arquivo errôneo. Se for esse o caso, um usuário não pode provar que ele realmente possui o NFT. Em suma, confiar em um sistema externo como o componente central (armazenamento) para um sistema NFT é vulnerável (WANG *et al.*, 2021).

- Anonimato/Privacidade: No estágio atual, o anonimato e a privacidade dos NFTs ainda são pouco estudados. A maioria das transações de NFT depende de sua plataforma Ethereum subjacente, que só oferece pseudo-anonimato em vez de anonimato estrito ou privacidade. Os usuários podem ocultar parcialmente suas identidades se os links entre suas identidades reais e os endereços correspondentes forem desconhecidos pelo público. Caso contrário, todas as atividades dos usuários sob o endereço exposto são observáveis. As soluções existentes para preservação da privacidade (por exemplo, criptografia homomórfica , prova de conhecimento zero, assinatura em anel, computação multipartidária) ainda não foram aplicadas aos esquemas relacionados ao NFT devido a suas primitivas criptográficas complicadas e suposições de segurança. Semelhante a outros tipos de sistemas baseados em blockchain, diminuir os custos computacionais caros se torna a chave para implementar esquemas promissores de privacidade (WANG *et al.*, 2021).

### 2.5.2.3 Questões de Governança

Semelhante às situações da maioria das criptomoedas, os NFTs também enfrentam as barreiras como a gestão rigorosa do governo. Por outro lado, como regular adequadamente essa tecnologia nascente com o mercado correspondente também é um desafio. Discutimos duas questões típicas de ambos os lados (WANG *et al.*, 2021):

- Armadilhas Legais: Os NFTs enfrentam questões legais e políticas em uma ampla gama de áreas (WANG *et al.*, 2021). As áreas potencialmente preocupadas cobrem commodities, transações transfronteiriças, dados KYC (Conheça Seu Cliente), etc. É importante entender o escrutínio regulatório e a litigação antes de entrar nas trilhas NFT. Em alguns países, como Índia e China, a situação legal é rigorosa para criptomoedas, e também para vendas de NFT. Trocar, negociar, vender ou comprar NFTs tem que superar as dificuldades de governança.

Legalmente, os usuários só podem negociar derivativos em bolsas autorizadas, como ações e commodities, ou trocar tokens com alguém pessoa a pessoa. Vários países, como Malta e França, estão tentando implementar leis adequadas com o objetivo de regular o serviço de ativos digitais. Em outros lugares, as questões são resolvidas usando leis existentes. Eles exigem que os compradores sigam termos complexos ou até mesmo contraditórios. Portanto, realizar a devida diligência é uma necessidade antes de investir tokens sérios em NFTs (WANG *et al.*, 2021).

- Questões de Propriedade Tributável: Produtos relacionados à propriedade intelectual (incluindo artes, livros, nomes de domínio, etc.) são tratados como propriedade tributável sob o atual quadro legal. No entanto, as vendas baseadas em NFT ficam fora desse escopo. Embora poucos países, como os EUA (serviço de receita interna, IRS), tributem as criptomoedas como propriedade, a maioria das áreas em todo o mundo ainda não considerou isso. Isso pode aumentar muito os crimes financeiros sob o disfarce de negociação de NFT.

Os governos adorariam tornar a venda de NFTs confiável com consequências fiscais. Especificamente, os participantes individuais devem ter a responsabilidade fiscal sobre quaisquer ganhos de capital que estejam relacionados às propriedades NFT. Além disso, trocas de NFT por NFT, NFT por IP e Eth por NFT (ou vice-versa) devem ser tributadas. Além disso, para propriedades de alto lucro, ou colecionáveis, uma faixa de imposto mais alta deve ser aplicada. Assim, as negociações relacionadas a NFT são sugeridas para buscar mais conselhos de departamentos fiscais profissionais após discussões profundas (WANG *et al.*, 2021).

#### 2.5.2.4 Questões de Extensibilidade

A extensibilidade dos esquemas de NFT é dupla. A primeira é enfatizar se um sistema pode interagir com outros ecossistemas. A segunda se concentra em se os sistemas NFT podem obter atualizações quando a versão atual fica para trás (WANG *et al.*, 2021).

- Interoperabilidade de NFT (cross-chain): Os ecossistemas de NFT existentes estão isolados uns dos outros. Os usuários, uma vez que selecionaram um tipo de produto, só podem vendê-los/comprá-los/negociá-los dentro do mesmo ecossistema/rede. Isso se deve à razão de sua plataforma blockchain subjacente. A interoperabilidade e a comunicação cross-chain são sempre os obstáculos para a ampla adoção de DApps. As comunicações cross-chain só podem ser implementadas com a ajuda de partes externas confiáveis. A propriedade de descentralização, desta forma, foi inevitavelmente perdida até certo ponto. Mas, felizmente, a maioria dos projetos relacionados ao NFT adota o Ethereum como

sua plataforma subjacente. Isso indica que eles compartilham uma estrutura de dados semelhante e podem trocar sob as mesmas regras (WANG *et al.*, 2021).

- **NFTs Atualizáveis:** As blockchains transitórias atualizam seus protocolos por meio de soft forks (modificações menores que são compatíveis para frente) e hard forks (modificações significativas que podem entrar em conflito com os protocolos anteriores). Uma discussão formal foi fornecida em afirmando as dificuldades e compensações ao aplicar as atualizações a uma blockchain existente. Apesar de usar o modelo genérico, uma nova versão ainda enfrenta requisitos rigorosos, como tolerar comportamentos adversários específicos e permanecer online durante o processo de atualização. Os esquemas de NFT dependem fortemente de suas plataformas subjacentes e se mantêm consistentes com elas. Embora os dados sejam frequentemente armazenados em componentes separados (como o sistema de arquivos IPFS), a lógica mais importante e o token ainda são registrados na cadeia. Atualizar adequadamente o sistema com melhorias será uma necessidade (WANG *et al.*, 2021).

### 3 TRABALHOS CORRELATOS

A tecnologia de NFTs na blockchain da hyperledger ainda é muito nova e isto ficou evidente durante a realização da revisão bibliográfica sistemática. Quando fala-se de Badges na hyperledger tomando como premissa que é derivado da tecnologia de NFT e junto a isso o benefício de aplicar essa tecnologia no sistema educacional pela Fabric, são poucos os artigos que abordam esta temática de forma completa, por estes motivos optou-se por analisar artigos que abordassem cada uma das temáticas de forma separada, representando o real estado da arte.

Ao todo, foram produzidos resumos de cinco trabalhos, incluindo "A New Decentralized Certification Verification Privacy Control Protocol"(SALEH; GHAZALI; IDRIS, 2021), "Educational Applications of Non-Fungible Token (NFT)"(CHIH-HUNG WU, 2023), "Development of a Blockchain-Based Application for Digital Certificates in Education"(NIKOLIĆ *et al.*, 2022), "Non-fungible tokens, decentralized autonomous organizations, Web 3.0, and the metaverse in education: From university to metaversity"(TOLE SUTIKNO, 2023), e "FabAsset: Unique Digital Asset Management System for Hyperledger Fabric"(HONG *et al.*, 2020). Esses trabalhos foram peças centrais para a produção deste trabalho.

#### 3.1 A NEW DECENTRALIZED CERTIFICATION VERIFICATION PRIVACY CONTROL PROTOCOL

Este artigo, intitulado "A New Decentralized Certification Verification Privacy Control Protocol", foi escrito por Omar S. Saleh, Osman Ghazali e Norbik Bashah Idris. O estudo discute o uso da tecnologia blockchain na verificação de certificados acadêmicos e propõe um novo protocolo descentralizado de controle de privacidade para verificação de certificados.

Os certificados acadêmicos são uma convenção social que oferece um meio de atestar novos conhecimentos obtidos por uma pessoa ou entidade sobre uma pessoa ou entidade. A falsificação de certificados é uma prática comum que prejudica o investimento e a confiança nos sistemas de ensino superior. A blockchain foi introduzida para melhorar o processo de verificação de certificados acadêmicos e surgiu como uma maneira potencial de autenticar documentos e como uma ferramenta eficaz para combater fraudes e uso indevido de documentos.

No entanto, a preservação da privacidade foi um desafio na maioria das soluções existentes. A privacidade indica que o certificado protege tanto a identidade quanto as informações. Portanto, é proposto um novo protocolo de controle de privacidade descentralizado para verificação de certificação. O protocolo proposto pode ser usado para emissão e verificação de certificados educacionais, mantendo a privacidade e a confidencialidade tanto no nível de rede (nível de ministérios, universidades e estudantes) quanto no nível de dados.

A solução descentralizada foi implementada usando Hyperledger Fabric como infraestrutura e Javascript como linguagem de contrato. As características da blockchain, como imutabilidade, transparência e confiabilidade, são valiosas não apenas em criptomoedas, mas também em vários outros campos, levando ao desenvolvimento de aplicações baseadas em blockchain em áreas como governo, educação, saúde e ciência.

A pesquisa estabeleceu e abordou o valor da tecnologia blockchain na autenticação de certificados educacionais, bem como as complexidades de sua implementação na educação. Um dos principais problemas identificados no processo de verificação de certificados baseado em blockchain é a proteção da privacidade. A privacidade e a confidencialidade garantem que a identidade e as informações presentes no certificado estejam seguras. Portanto, foi proposto um novo Protocolo Descentralizado de Controle de Privacidade para Verificação de Credenciais.

O protocolo proposto visa proteger a privacidade e a confidencialidade no nível da rede, envolvendo ministérios, universidades e estudantes. O protocolo será introduzido e implementado em instituições educacionais selecionadas para trabalhos futuros.

### 3.2 EDUCATIONAL APPLICATIONS OF NON-FUNGIBLE TOKEN (NFT)

O artigo "Educational Applications of Non-Fungible Token (NFT)", escrito por Chih-Hung Wu e Chien-Yu Liu, explora o potencial das aplicações educacionais de NFTs no setor de educação. Com a emergência dos NFTs na tecnologia blockchain, as instituições de ensino podem utilizar NFTs para recompensar os alunos por meio do processamento automático de informações de transações e processos de compra e venda de material escolar usando a tecnologia de contratos inteligentes. Isso permite o estabelecimento de níveis de reconhecimento e incentiva os alunos a receberem recompensas de reconhecimento em NFT.

De acordo com a Pirâmide de Aprendizado Taxonômica, o aprendizado através de experiências práticas desempenha um papel crucial na atração do interesse dos alunos. Neste estudo, os autores analisam o potencial do uso de NFTs na educação e as aplicações atuais dos NFTs na sociedade. Eles conduzem um estudo de caso e realizam uma investigação preliminar dos tipos de aplicações NFT na indústria educacional. Em seguida, analisam diferentes setores educacionais usando análise individual combinada com análise SWOT para entender o impacto, o valor e os desafios das aplicações de NFT.

Os resultados revelam 10 aplicações educacionais de NFTs: livros didáticos; microcertificados; históricos escolares e registros; bolsas de estudo e direitos; masterclasses e criação de conteúdo; experiências de aprendizado; registro e coleta de dados; patentes, inovação e pesquisa; arte; pagamento e depósito. Por fim, o artigo discute maneiras de reduzir o impacto negativo dos NFTs educacionais no ambiente sustentável.

### 3.3 DEVELOPMENT OF A BLOCKCHAIN-BASED APPLICATION FOR DIGITAL CERTIFICATES IN EDUCATION

O artigo "Development of a Blockchain-Based Application for Digital Certificates in Education" discute a criação de um sistema de gerenciamento escolar baseado em blockchain conhecido como "Eternal Digital Certificate". Este sistema tem como objetivo principal armazenar informações sobre eventos escolares e seus participantes, além de emitir certificados para esses eventos.

A plataforma blockchain escolhida para armazenar essas informações é a Polygon Supernets, que é uma rede descentralizada de blockchains. Os certificados são emitidos como NFTs para os estudantes que completaram com sucesso todos os cursos de um evento e são mantidos em suas carteiras pessoais. Esses certificados não podem ser vendidos ou transferidos para outra carteira.

O uso de um sistema blockchain para armazenar informações de educação e carreira de uma pessoa simplifica o processo de análise de dados, tornando-se útil na avaliação de candidatos a empregos, bolsas e outras situações que exijam a classificação de pessoas com base em critérios que incluem o nível de educação. Além disso, como o sistema é descentralizado, não há necessidade de terceiros para verificar os certificados. Isso pode ser especialmente útil para estudantes que se transferirem de uma instituição para outra, pois facilita o processo de verificação e equivalência de disciplinas.

### 3.4 NON-FUNGIBLE TOKENS, DECENTRALIZED AUTONOMOUS ORGANIZATIONS, WEB 3.0, AND THE METAVERSE IN EDUCATION: FROM UNIVERSITY TO METAVERSITY

O artigo "Non-fungible tokens, decentralized autonomous organizations, Web 3.0, and the metaverse in education: From university to metaversity" discute o impacto das tecnologias NFTs, DAOs, Web 3.0 e metaverso na educação. O blockchain permite a utilização de NFTs para validar diplomas universitários e históricos escolares, e as DAOs estão sendo implementadas para automatizar e autenticar cursos e certificados. A Web 3.0 é uma evolução da internet que torna-a legível por máquinas, enquanto o metaverso oferece experiências imersivas e interativas aos alunos. A "metaversidade" é uma referência a um campus virtual que fornece uma experiência de metaverso para a educação, permitindo que os alunos participem de aulas e atividades educacionais em realidade virtual.

### 3.5 FABASSET: UNIQUE DIGITAL ASSET MANAGEMENT SYSTEM FOR HYPER-LEDGER FABRIC

O artigo "FabAsset: Unique Digital Asset Management System for Hyperledger Fabric", escrito por Sangwon Hong, Yoongdo Noh, Jeyoung Hwang e Chanik Park, aborda

o gerenciamento de ativos digitais únicos na plataforma de blockchain permissionada Hyperledger Fabric. O artigo identifica a necessidade de suporte a NFTs na plataforma, visto que a versão 2.0.0 alpha do Hyperledger Fabric introduziu o FabToken, que suporta apenas tokens fungíveis (FTs).

Para abordar essa lacuna, os autores apresentam o FabAsset, um sistema de gerenciamento de ativos digitais únicos para o Hyperledger Fabric. O FabAsset avança o XNFT (modelo extensível de NFT para Fabric), modularizando seus componentes em chaincode (ou seja, contrato inteligente para o Fabric) e SDK para construir um sistema completo para NFTs.

Os autores também demonstram um protótipo de serviço de assinatura descentralizado para validar a utilidade do FabAsset. O objetivo do artigo é aproveitar o potencial dos NFTs no contexto das blockchains empresariais e expandir as capacidades do Hyperledger Fabric para incluir o suporte a esses ativos digitais únicos.



## 4 PROPOSTA

### 4.1 INTRODUÇÃO

Este capítulo destina-se a discutir a proposta central deste TCC, que é a implementação de uma nova funcionalidade no projeto "Jornada do Estudante". A funcionalidade proposta é a tokenização, ou seja, a utilização da blockchain Hyperledger para produzir NFTs representando *badges* no contexto educacional.

A inspiração para esta proposta vem, inicialmente, do trabalho correlato "FabAsset: Unique Digital Asset Management System for Hyperledger Fabric"(HONG *et al.*, 2020). Este trabalho demonstra um protótipo que aproveita o potencial dos NFTs no contexto das blockchains empresariais, expandindo as capacidades do Hyperledger Fabric para incluir o suporte a esses ativos digitais únicos.

Além disso, uma inspiração significativa para a implementação do front-end e do processo de autenticação veio do TCC de Bruno Daniel Elias, "Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino"(ELIAS, 2023). O trabalho de Elias fornece um modelo valioso para a integração segura e eficiente de sistemas de autenticação, utilizando o acesso do gov.br, que é fundamental para a gestão de identidades digitais no contexto da nossa proposta.

Neste capítulo, exploraremos como essas capacidades podem ser utilizadas para realmente produzir esses ativos no contexto do projeto "Jornada do Estudante". Discutiremos os detalhes da implementação, os desafios esperados e os resultados potenciais desta proposta. A abordagem integrada, combinando as inovações do FabAsset com as práticas de autenticação e segurança de dados do trabalho de Elias, oferece uma base sólida para o desenvolvimento de um sistema robusto e eficaz no contexto educacional.

### 4.2 GAMIFICAÇÕES A SEREM IMPLEMENTADAS

A gamificação tem se mostrado uma estratégia eficaz para aumentar o engajamento e a motivação dos estudantes (BRASIL, 2023). Neste contexto, propomos a implementação de tokens ou *badges* que representem conquistas específicas no cenário educacional. Esses tokens, que serão implementados como NFTs na blockchain Hyperledger Fabric, servirão como uma representação tangível e imutável das conquistas dos estudantes.

As *badges* a seguir, que serão implementadas no nosso desenvolvimento, representam apenas alguns exemplos das possibilidades de gamificação no contexto educacional. Acreditamos que a implementação desses tokens pode trazer benefícios significativos para o engajamento e a motivação dos estudantes, além de fornecer uma representação tangível e imutável de suas conquistas.

### 4.2.1 Melhor Atleta de um Campeonato

Esta badge seria concedido ao estudante que se destacasse como o melhor atleta em um determinado campeonato esportivo. Ele serviria não apenas como um reconhecimento do talento e esforço do estudante, mas também como um incentivo para outros estudantes participarem e se esforçarem nos eventos esportivos.

### 4.2.2 Melhor Aluno da Disciplina no Semestre

Este token seria concedido ao estudante que obtivesse o melhor desempenho em uma disciplina específica em um determinado semestre. Este reconhecimento poderia incentivar os estudantes a se dedicarem mais aos seus estudos e a buscarem a excelência acadêmica.

### 4.2.3 Melhor Aluno do Curso na Formatura

Esta badge seria concedido ao estudante que se destacasse como o melhor aluno de um determinado curso. Este reconhecimento poderia servir como um incentivo para os estudantes se esforçarem para alcançar o melhor desempenho possível em seus cursos.

## 4.3 PRIVACIDADE DAS BADGES

A privacidade é uma consideração importante quando se trata de dados educacionais. Embora as badges representem conquistas que os estudantes possam querer compartilhar publicamente, também é importante reconhecer que algumas informações contidas nessas badges podem ser de natureza privada. Por exemplo, um estudante pode não querer que detalhes específicos sobre suas notas acadêmicas ou seu desempenho em determinadas atividades sejam publicamente acessíveis.

Nossa proposta leva em consideração essas preocupações de privacidade. Embora as badges sejam armazenadas de forma imutável na blockchain, o conteúdo específico dessas badges não precisa ser publicamente visível. Em vez disso, os estudantes terão a capacidade de controlar quais informações são tornadas públicas e quais são mantidas privadas.

Por exemplo, um estudante pode escolher tornar público o fato de que recebeu a badge de "Melhor Aluno da Disciplina Y do Ano XXXX", mas manter privadas as informações específicas sobre suas notas ou desempenho acadêmico que levaram à concessão dessa badge.

Desta forma, os estudantes podem desfrutar dos benefícios de ter suas conquistas reconhecidas e validadas através de NFTs, sem sacrificar sua privacidade. Acreditamos que este equilíbrio entre reconhecimento público e privacidade é crucial para o sucesso de nossa proposta.

#### 4.4 TRANSPORTE DE BADGES PARA BLOCKCHAINS PÚBLICAS

O transporte de badges para blockchains públicas é uma possível funcionalidade da nossa proposta. Isso permite que os estudantes tenham controle total sobre suas badges e possam compartilhá-las de maneira segura e verificável.

As badges serão inicialmente criadas e armazenadas na blockchain Hyperledger Fabric, que é uma blockchain privada e permissionada. Isso garante que apenas entidades autorizadas possam criar e emitir badges, mantendo a integridade e a confiabilidade do sistema.

Quando um estudante deseja transportar suas badges para uma blockchain pública, o processo é o seguinte:

1. **Solicitação de Transporte:** O estudante solicita o transporte de uma badge específica para uma blockchain pública. Esta solicitação é feita através de uma interface de usuário, que pode ser um aplicativo web ou móvel.
2. **Assinatura da Badge:** A entidade que emitiu a badge (por exemplo, a instituição de ensino) assina a badge com sua chave privada. Esta assinatura serve como uma prova de que a badge é autêntica e foi emitida por uma entidade autorizada.
3. **Criação do NFT:** A badge assinada é então transformada em um NFT na blockchain pública. Este NFT é associado à chave pública do estudante, garantindo que apenas o estudante tenha controle sobre ele.
4. **Verificação:** Qualquer pessoa que receba o NFT pode verificar sua autenticidade verificando a assinatura da badge. Isso pode ser feito usando a chave pública da entidade emissora, que pode ser facilmente obtida e verificada.

Este processo garante que as badges possam ser transportadas de forma segura para blockchains públicas, mantendo ao mesmo tempo a privacidade e o controle do estudante sobre suas próprias badges. Além disso, permite que as badges sejam verificadas por qualquer pessoa, aumentando a transparência e a confiabilidade do sistema.

#### 4.5 WORKFLOW DE GERAÇÃO DAS BADGES

A geração de badges é um processo que envolve várias etapas, desde a identificação da conquista que a badge representa até a sua emissão e registro na blockchain. Aqui está o fluxo de trabalho proposto para a geração das badges:

1. **Identificação da Conquista:** A primeira etapa é identificar a conquista que a badge vai representar. Isso pode ser o desempenho excepcional em uma disciplina específica, a vitória em um evento esportivo, ou qualquer outra conquista relevante no contexto educacional.

2. **Criação da Badge:** Uma vez identificada a conquista, a próxima etapa é criar a badge. Isso envolve o design da badge e a definição das informações que ela vai conter. As informações podem incluir o nome do estudante, a descrição da conquista, a data, entre outros.
3. **Assinatura da Badge:** A badge é então assinada pela instituição de ensino ou outra entidade autorizada. A assinatura serve como uma garantia de que a badge é autêntica e foi emitida por uma entidade confiável.
4. **Emissão da Badge:** A badge assinada é então emitida para o estudante. Isso pode ser feito através de uma interface de usuário, como um aplicativo web ou móvel.
5. **Registro na Blockchain:** Finalmente, a badge é registrada na blockchain Hyperledger. Isso envolve a criação de um novo NFT que representa a badge e está associado à chave pública do estudante.
6. **Verificação:** Após o registro da badge na blockchain, qualquer pessoa pode verificar a autenticidade da badge verificando a assinatura. Isso garante que as badges não possam ser falsificadas e que as conquistas dos estudantes possam ser verificadas de forma confiável.

Este fluxo de trabalho garante que as badges sejam geradas de forma segura e confiável, e que as conquistas dos estudantes sejam reconhecidas de forma transparente e verificável.

## 4.6 IMPLEMENTAÇÃO

A implementação desta proposta é um processo que envolve duas vertentes principais: o desenvolvimento de chaincodes e a criação de uma interface gráfica. Ambos são fundamentais para o sucesso do projeto, cada um desempenhando um papel único e complementar.

**Desenvolvimento de Chaincodes:** Os chaincodes, que são os contratos inteligentes na blockchain Hyperledger Fabric, formam a base do nosso sistema. Eles são projetados para definir as regras de criação, emissão e transferência de badges. Esses contratos garantem que todas as transações sejam realizadas conforme as normas estabelecidas, assegurando a autenticidade e a imutabilidade das badges. O desenvolvimento desses chaincodes exige proficiência na linguagem de programação Go, uma escolha popular para escrever chaincodes para a Hyperledger Fabric.

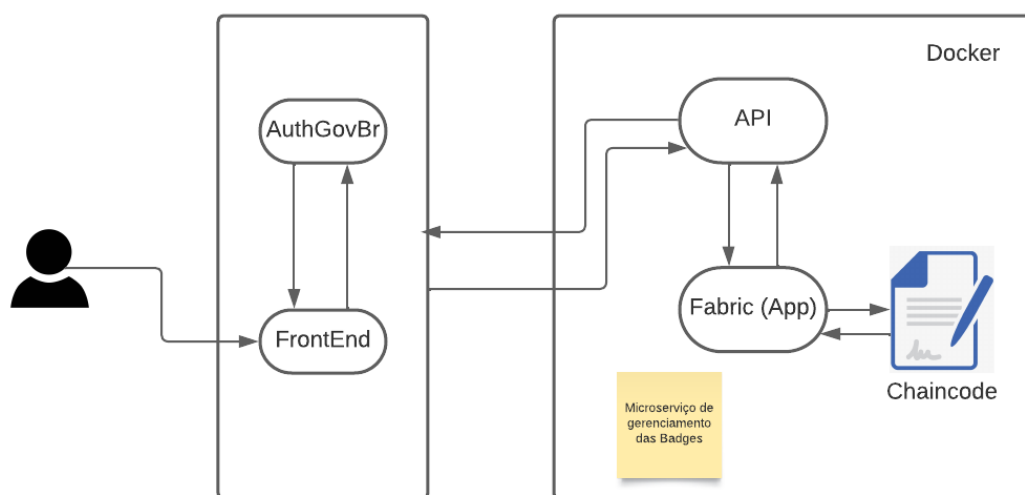
**Criação da Interface Gráfica:** Paralelamente, a interface gráfica representa o ponto de contato entre os usuários (estudantes e instituições de ensino) e a blockchain. Esta interface é projetada para ser intuitiva e amigável, permitindo que os usuários visualizem facilmente seus dados na blockchain, incluindo as badges. A acessibilidade é uma prioridade, garantindo que a interface possa ser utilizada eficazmente por todos,

independentemente do seu nível de conhecimento técnico. Para o desenvolvimento desta interface, utilizaremos a SDK do Node para Hyperledger Fabric, que oferece ferramentas para facilitar a interação com a blockchain.

Portanto, a implementação desta proposta envolverá tanto o desenvolvimento de chaincodes quanto a criação de uma interface gráfica. Ambos os componentes serão desenvolvidos em paralelo, para garantir que funcionem de forma integrada e proporcionem uma experiência de usuário suave e eficaz. No desenvolvimento deste projeto, adotamos um modelo arquitetônico e funcional, ilustrado na Figura 3, que serve como a espinha dorsal do nosso sistema. A arquitetura do modelo é composta por vários componentes chave, cada um desempenhando um papel vital no funcionamento geral do sistema:

Temos o usuário, que se conecta com o front-end e que faz requisição para se autenticar com o GovBr, o qual habilita credenciais para o acesso desse usuário ao sistema. Ao acessar o front autenticado o sistema se comunica com a Application Programming Interface (API) que fornece acesso aos métodos providos pelas aplicações, e essa API se comunica com a aplicação APP permitindo uma integração eficiente e uma comunicação fluida entre diferentes partes do sistema. APP, implementada a partir do SDK do Node para Hyperledger Fabric, faz requisições ao chaincode para recuperar *badges* criadas. Esse conjunto de quatro serviços é comumente utilizado para outras chaincodes no projeto Jornada do Estudante.

Figura 3 – Modelo Proposto



Fonte: Elaborado pelo autor

#### 4.7 CONTRIBUIÇÕES DA PROPOSTA

A proposta apresentada neste trabalho traz várias contribuições significativas, tanto para o projeto Jornada do Estudante quanto para o campo mais amplo da educação e da

tecnologia blockchain. Entre elas estão:

1. **Incentivo à Participação dos Alunos:** Ao implementar badges como NFTs para reconhecer e recompensar as conquistas dos alunos, esperamos incentivar a participação ativa dos alunos. Isso pode se manifestar de várias maneiras, desde o aumento do envolvimento nas atividades acadêmicas e esportivas até a melhoria do desempenho acadêmico. Além disso, ao registrar as *soft skills* dos alunos, como liderança, trabalho em equipe e resolução de problemas, podemos ajudar a destacar essas habilidades importantes que muitas vezes são subestimadas no ambiente acadêmico tradicional.
2. **Contribuição para o Projeto Jornada do Estudante:** A implementação de NFTs no projeto Jornada do Estudante representa uma inovação significativa. Ao aproveitar a tecnologia blockchain, podemos melhorar a segurança, a transparência e a verificabilidade das conquistas dos alunos. Isso pode aumentar a confiança no projeto Jornada do Estudante e melhorar sua eficácia como uma ferramenta para apoiar o desenvolvimento dos alunos.
3. **Avanço da Tecnologia Blockchain na Educação:** Ao implementar NFTs no contexto educacional, estamos explorando novas maneiras de aplicar a tecnologia blockchain na educação. Isso pode abrir caminho para futuras inovações e contribuir para o desenvolvimento da tecnologia blockchain como uma ferramenta valiosa para melhorar a educação.

## 5 PROTOTIPO

### 5.1 INTRODUÇÃO

Neste capítulo, detalharemos o protótipo desenvolvido para a implementação de badges digitais como ferramentas de gamificação no ensino superior, empregando a tecnologia blockchain Hyperledger Fabric. Este protótipo, uma extensão inovadora do projeto "Jornada do Estudante", foca na criação e gerenciamento de NFTs que representam as conquistas educacionais dos alunos.

O desenvolvimento deste protótipo foi realizado com uma abordagem integrada, combinando tecnologias de front-end modernas com processos de chaincode robustos na blockchain Hyperledger. A chaincode, crucial para o funcionamento da nossa solução blockchain, foi escrita em Go. Esta linguagem foi escolhida por sua eficiência e adequação ao desenvolvimento de chaincodes, permitindo-nos definir regras de negócio precisas e lógica de transação para os NFTs. Essa implementação assegura operações seguras e confiáveis na blockchain, essenciais para a emissão e gerenciamento das badges digitais.

Para a infraestrutura, utilizamos servidores virtuais, otimizando a conectividade e interação com a blockchain. A interface do usuário foi desenvolvida com tecnologias atuais, como React.js, para garantir uma experiência de usuário intuitiva e envolvente.

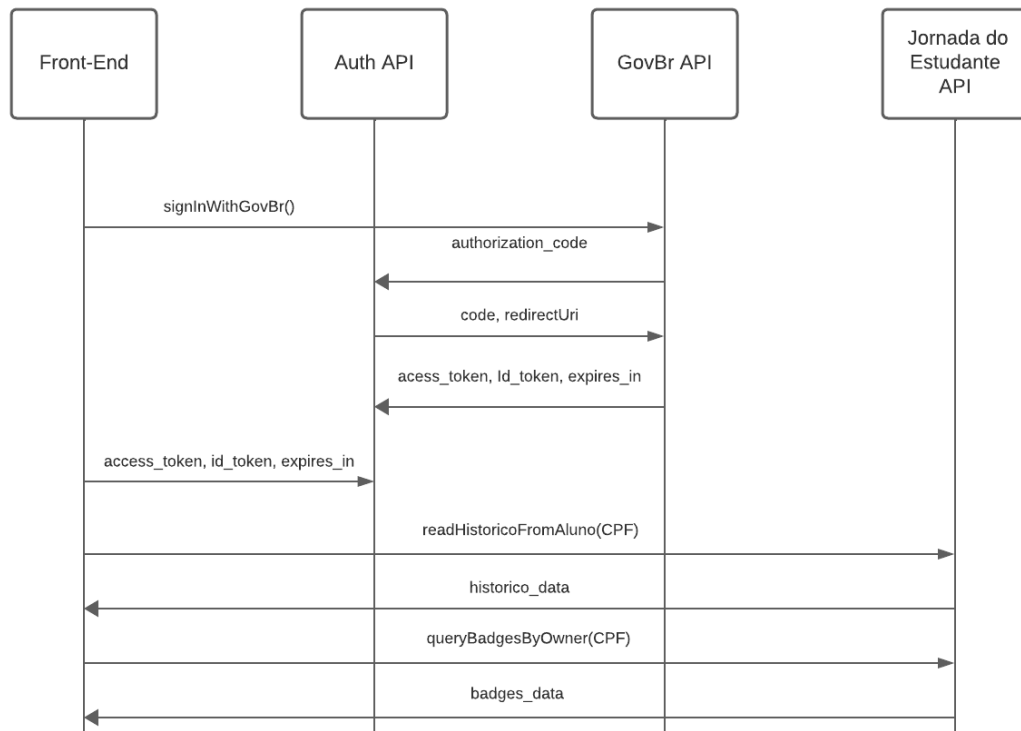
Um aspecto fundamental deste protótipo é a integração com o sistema de autenticação do gov.br, inspirado pelo trabalho de Bruno Daniel Elias em seu TCC "Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino"(ELIAS, 2023). Implementamos uma API de autenticação customizada, utilizando o Login Único do gov.br, para autenticar os usuários de forma segura e vincular suas identidades digitais aos registros na blockchain.

Neste capítulo, além de apresentar a configuração da rede Hyperledger e a implementação da chaincode em Go, também discutiremos a arquitetura e o fluxo de trabalho do sistema. Para uma compreensão visual, incluímos um fluxograma do front-end (ver Figura 4) e do chaincode (ver Figura 5), que ilustra o processo de interação entre as diferentes componentes do sistema, desde a autenticação do usuário até a emissão e gerenciamento das badges digitais.

Discutiremos os desafios técnicos, as soluções adotadas e as inovações implementadas, destacando a importância da chaincode e a influência do trabalho de Bruno Daniel Elias no desenvolvimento do nosso sistema de autenticação.

Finalizaremos com uma discussão sobre os resultados esperados deste protótipo, ressaltando seu potencial para aumentar o engajamento dos alunos e enriquecer o processo educacional através da gamificação e da tecnologia blockchain.

Figura 4 – Fluxograma Front-end



Fonte: Elaborado pelo autor

## 5.2 CHAINCODE

No desenvolvimento do chaincode do prototipo em Go, foi projetado para o gerenciamento de badges no formato de NFTs na plataforma Hyperledger Fabric. O chaincode é uma peça central no sistema de blockchain, responsável por definir as regras de negócio e a lógica de manipulação dos dados. Neste caso, o foco é na criação, transferência, revogação e consulta de badges, que representam conquistas ou credenciais digitais.

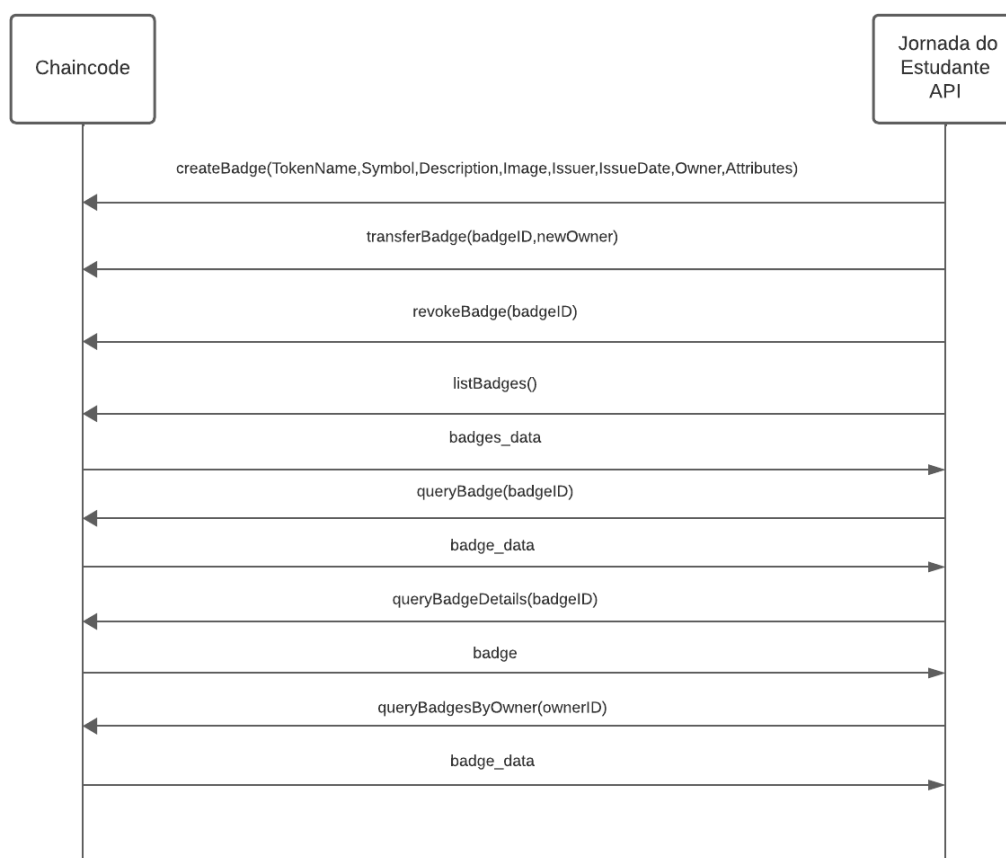
### 5.2.0.1 Estrutura do Chaincode

O chaincode é estruturado em torno de várias componentes principais:

- **Definição da Estrutura Badge** A estrutura Badge é definida para representar um NFT. Ela inclui campos como Owner, TokenType, TokenName, Description, BasicDescription, IpfsImage, IssuerCpf, IssueDate e ExtraAttributes, que armazenam informações relevantes sobre cada badge.
- **SmartContract Struct** A estrutura SmartContract serve como a espinha dorsal do chaincode, dentro da qual todas as funções operacionais são definidas.
- **Funções de Inicialização e Invocação** As funções Init e Invoke são implementadas para atender aos requisitos do Hyperledger Fabric. Init é usada para



Figura 5 – Fluxograma Chaincode Badge



Fonte: Elaborado pelo autor

qualquer inicialização necessária durante a instanciação do chaincode, enquanto Invoke roteia as chamadas para diferentes funções com base no nome da função fornecido.

### 5.2.0.2 Funções Principais do Chaincode

O chaincode inclui várias funções para gerenciar o ciclo de vida das badges:

- **Criação de Badge (handleCreateBadge)** Esta função valida os argumentos de entrada e invoca a função createBadge para criar uma nova badge no ledger. A função verifica se a badge já existe para evitar duplicatas.
- **Transferência de Badge (handleTransferBadge)** Implementa a lógica para transferir a propriedade de uma badge para outro usuário, atualizando o campo Owner da badge.
- **Revogação de Badge (handleRevokeBadge)** Permite a revogação de uma badge, o que é feito atualizando um atributo específico (revoked) na estrutura da badge.

- **Listagem de Badges (`handleListBadges`)** Fornece uma lista de todas as badges emitidas, iterando sobre os registros armazenados no ledger.
- **Consulta de Badge (`handleQueryBadge`)** Retorna detalhes de uma badge específica com base em seu identificador.
- **Consulta de Detalhes de Badge (`handleQueryBadgeDetails`)** Fornece detalhes mais aprofundados de uma badge específica.
- **Consulta de Badges por Proprietário (`handleQueryBadgesByOwner`)** Retorna todas as badges associadas a um determinado proprietário.

### 5.2.0.3 Implementação e Lógica de Negócios

Cada função do chaincode é cuidadosamente projetada para atender a um aspecto específico da gestão de badges:

- **Criação de Badge** A função `createBadge` é um exemplo de como o chaincode interage com o ledger do Hyperledger Fabric. Ela realiza a serialização da estrutura da badge para JSON e a armazena no ledger usando uma chave composta.
- **Transferência de Badge** Esta função destaca a mutabilidade controlada de registros em um sistema blockchain. Ao transferir a propriedade de uma badge, a integridade e o rastreamento da badge são mantidos.
- **Revogação de Badge** A função de revogação ilustra como as regras de negócio podem ser implementadas em um chaincode. A revogação não exclui a badge, mas altera seu estado, preservando o histórico.
- **Consultas** As funções de consulta demonstram a capacidade de interagir e recuperar dados do ledger. Elas são essenciais para verificar o estado e a propriedade das badges.

### 5.2.0.4 Considerações de Segurança e Melhores Práticas

O chaincode incorpora várias práticas recomendadas:

- **Validação de Argumentos** Cada função realiza verificações dos argumentos para garantir a integridade das operações.
- **Manipulação de Erros** O chaincode lida consistentemente com erros, retornando mensagens descritivas para facilitar a depuração e a manutenção.

Através do uso de Hyperledger Fabric e da linguagem Go, foi possível criar um chaincode adequado para a emissão, transferência e gerenciamento de badges como NFTs.

### 5.3 FRONT-END

No desenvolvimento do front-end do nosso protótipo, focamos em proporcionar uma experiência de usuário intuitiva e agradável, essencial para a interação eficaz com o sistema. O design foi elaborado seguindo as diretrizes do Design System GovBr (BRASIL, 2023). Nosso objetivo era criar uma interface responsiva e de fácil navegação, com uma estética moderna que atendesse às expectativas e necessidades dos usuários contemporâneos.

Para alcançar esse objetivo, escolhemos utilizar tecnologias modernas e amplamente adotadas no desenvolvimento do front-end. React.js foi a escolha principal devido à sua flexibilidade, eficiência e o suporte de uma ampla comunidade. Esta tecnologia nos permitiu criar uma interface dinâmica e reativa, que responde de maneira fluida às interações dos usuários. Além disso, a integração de frameworks e bibliotecas adicionais, como Styled-Components para o layout e Axios para as requisições HTTP, foi crucial para a eficiência do desenvolvimento e a robustez do sistema. Styled-Components facilitou a criação de um layout consistente e responsivo, enquanto Axios aprimorou a gestão das comunicações de rede, assegurando uma interação suave com o back-end.

Combinando essas tecnologias, conseguimos desenvolver um front-end que não só é visualmente atraente, mas também funcional e fácil de usar. Acreditamos que esta abordagem não apenas melhora a experiência do usuário, mas também desempenha um papel vital na aceitação e satisfação do usuário, fatores cruciais para o sucesso de qualquer aplicação digital no ambiente educacional atual.

#### 5.3.1 Organização do código

A organização do código front-end foi planejada para garantir eficiência e facilidade de manutenção. Seguindo a Folder Architecture do React (ROBIN WIERUCH, 2017), estruturamos o código em várias pastas, cada uma com um propósito específico:

- **/src:** O núcleo do código-fonte, organizado em subpastas para facilitar a manutenção e expansão.
- **/src/@types:** Armazena definições de tipos para bibliotecas JavaScript de terceiros.
- **/src/assets:** Contém recursos como imagens e ícones, essenciais para a estética do projeto.
- **/src/components:** Inclui componentes React reutilizáveis, fundamentais para a construção das páginas e elementos da interface.
- **/src/pages:** Armazena os arquivos relacionados às páginas da aplicação, com cada arquivo correspondendo a uma rota específica.
- **/src/styles:** Centraliza os estilos gerais e os temas da aplicação.

- **/src/utills:** Contém funções e constantes úteis, utilizadas em várias partes do projeto.

### 5.3.2 Arquivos da Raiz do Projeto

Os arquivos na raiz do projeto desempenham um papel crucial na configuração e implantação do sistema:

#### 5.3.2.1 Arquivo *main.tsx*

Este arquivo é o ponto de entrada da aplicação React, responsável por renderizar o componente principal na página.

#### 5.3.2.2 Arquivo *app.tsx*

Define a função `App()`, que estrutura os componentes React e gerencia a navegação baseada em rotas com o `BrowserRouter`.

#### 5.3.2.3 Arquivo *Router.tsx*

Esse arquivo é essencial para definir as rotas públicas e privadas da aplicação, utilizando a biblioteca `react-router-dom`.

### 5.3.3 Páginas da Aplicação

As páginas da aplicação foram desenvolvidas utilizando o Design System do Governo Brasileiro, garantindo uma interface com alta usabilidade e qualidade visual. Este sistema oferece uma padronização eficaz para as interfaces dos serviços públicos digitais, além de orientações claras para o desenvolvimento, contribuindo para a redução do tempo de desenvolvimento e manutenção.

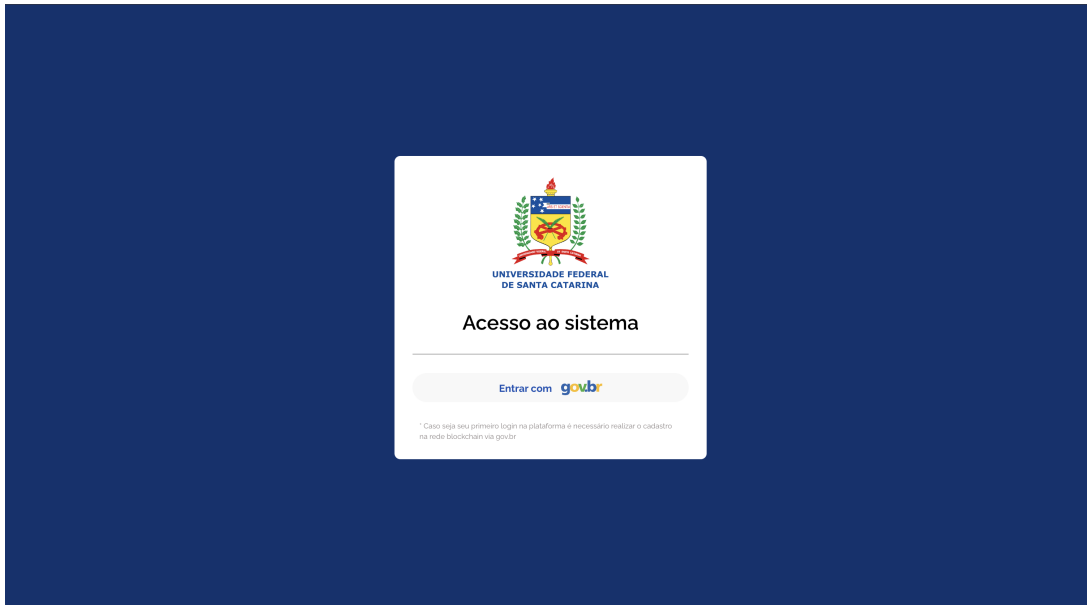
#### 5.3.3.1 Página de Login

A página de login do nosso protótipo, ilustrada na Figura 6, é um exemplo de simplicidade e eficiência. Baseada em um componente funcional React chamado `SignIn`, a página é projetada para facilitar o acesso à rede blockchain. O elemento central da página é um botão que inicia o processo de login utilizando o sistema de autenticação do gov.br.

Ao clicar no botão, o método `handleGovBrSignIn()` é acionado, desencadeando uma requisição GET para a API de autorização do Governo Federal Brasileiro. Esta requisição, direcionada à versão de homologação (staging), inclui uma série de parâmetros essenciais para a autenticação segura:

- **responseType:** Indica que um código de autorização deve ser retornado.
- **clientId:** Identifica a aplicação solicitante, neste caso, `systemas.homologacao.ufsc.br`.

Figura 6 – Página de Login



Fonte: Elaborado pelo autor

- **scope:** Define o escopo de acesso, incluindo informações básicas do perfil do usuário e dados de autenticação.
- **redirect uri:** Especifica a URI de redirecionamento para a resposta da requisição, neste caso, <https://govbr.labsec.ufsc.br:3000/redirect>
- **nonce e state:** Valores aleatórios usados para proteger a requisição contra ataques Cross-Site Request Forgery (CSRF).

Durante a requisição, uma nova janela é aberta no navegador, direcionando o usuário para o serviço de autenticação do governo brasileiro. Aqui, o usuário pode inserir seus dados de login. No ambiente de desenvolvimento, é necessário seguir um procedimento específico para criar uma nova conta, incluindo a inserção de um CPF válido, a criação de uma senha e a validação através de email ou SMS.

Após a autenticação bem-sucedida no ambiente de desenvolvimento, o usuário pode acessar o sistema com o CPF e a senha definidos. Este processo não só garante a segurança da autenticação, mas também integra o sistema de forma eficiente com a infraestrutura de autenticação do governo, proporcionando uma experiência de usuário coesa e segura.

### 5.3.3.2 Página de Home

A página de Home, conforme ilustrada na Figura 7, é construída utilizando um componente funcional React denominado Home. Este componente é encarregado de renderizar a página principal da aplicação. Ele faz uso do hook `useLocation()` do React Router para capturar dados transmitidos via URL após o redirecionamento de autenticação.

ção. Adicionalmente, a biblioteca `jwt-decode` é importada para decodificar os tokens de autenticação.

Figura 7 – Página de Home



Fonte: Elaborado pelo autor

Dentro do componente Home, é definida uma interface `DecodedIdToken` que encapsula as informações do usuário presentes no token decodificado, como nome, e-mail, CPF e data de expiração do token. Além disso, o componente implementa uma função `handleLogout()`. Esta função realiza uma solicitação ao servidor de autenticação para deslogar o usuário, redirecionando-o para a página de login sob duas condições específicas: se o tempo de expiração do token for zero ou se o token não estiver presente.

A página de Home também integra-se com a API do Jornada do Estudante. Isso é feito através do método `getHistoricosFromCpf(cpf)`, onde o CPF fornecido é o mesmo recebido pelo token do GovBr. Essa função envia uma requisição HTTP para a rota `/api/academicRecords/read/readHistoricosFromAluno`. Com isso, é possível obter uma variedade de dados acadêmicos do usuário autenticado, demonstrando a viabilidade da integração entre o GovBr e a Jornada do Estudante, mas deixando claro que no presente trabalho utilizamos dados mockados para conseguirmos representar somente o necessário.

Além disso, a página de Home agora inclui a funcionalidade `getBadgesFromCPF(cpf)`. Esta função é responsável por interagir com o contrato de NFT, enviando requisição HTTP para a rota `/api/badges/read/queryBadgesByOwner` para recuperar dados relacionados às conquistas acadêmicas do aluno, representadas como NFTs. Ao fornecer o CPF do aluno, a função consulta o contrato inteligente no blockchain, retornando informações detalhadas sobre as badges (NFTs) associadas ao aluno. Isso não apenas enriquece a experiência do usuário com informações relevantes e personalizadas, mas também demonstra a integração eficaz entre sistemas tradicionais de gerenciamento de dados acadêmicos e tecnologias emergentes como blockchain e NFTs.

## 5.4 INTEGRAÇÃO COM A BLOCKCHAIN JORNADA DO ESTUDANTE

A integração com a blockchain Jornada do Estudante foi um aspecto crucial no desenvolvimento deste trabalho. Esta seção descreve os procedimentos e comandos adotados para configurar e executar os diferentes componentes e serviços envolvidos na integração. A API, a aplicação, e o chaincode foram executados dentro do ambiente do projeto, seguindo passos similares a outros conjuntos de código.

### 5.4.1 Configuração do Ambiente de Desenvolvimento

Inicialmente, foi necessário estabelecer um ambiente de desenvolvimento local utilizando Docker. Para assegurar um ambiente limpo e organizado, foram utilizados os seguintes comandos:

- **Limpeza de Contêineres e Imagens Docker:**

- `docker rm -f $(docker ps -a -q)`: Remove todos os contêineres existentes.
- `docker system prune -a`: Limpa todas as imagens Docker não utilizadas.

### 5.4.2 Construção e Execução da Rede Blockchain

- **Construção da Imagem Docker:**

- Utilizando o Minifabric, a imagem `labsec/minifabacadbloc` foi construída com o comando `docker build -t labsec/minifab-acadbloc ..`

- **Inicialização da Rede:**

- Com o comando `./minifab up -e true`, a rede foi iniciada com configuração avançada.

### 5.4.3 Instalação e Inicialização dos Chaincodes

- **Chaincodes Utilizados:**

- `./minifab ccup -n badges`

### 5.4.4 Inicialização dos Aplicativos

- **Aplicativos e Comandos Correspondentes:**

- `./minifab appbadges` para iniciar o aplicativo "appbadges".
- Monitoramento dos logs com `docker logs appbadges -f`.

### 5.4.5 Inicialização da API

- **Comando Docker Compose:**

- Utilização de `docker compose up -build -d apibadges` na pasta raiz do projeto para construir e iniciar os contêineres especificados no arquivo de composição.

- **Verificação de Logs:**

- Monitoramento dos contêineres `backend-tcc-apibadges-1` com `docker logs backend-tcc-ap`

## 5.5 DESAFIOS

Durante o desenvolvimento do protótipo enfrentamos vários desafios significativos. Estes desafios não apenas testaram nossa capacidade técnica e criatividade, mas também forneceram entendimentos valiosos para futuras iterações do projeto.

### 5.5.1 Compreensão e Implementação da Hyperledger Fabric

Um dos principais desafios foi a compreensão e implementação da Hyperledger Fabric. A complexidade desta tecnologia blockchain exigiu um investimento considerável de tempo para entender suas nuances, especialmente no que diz respeito ao acesso e configuração das chaincodes. A necessidade de liberação de portas e máquinas externas para garantir o funcionamento adequado das chaincodes adicionou uma camada extra de complexidade ao processo.

### 5.5.2 Autenticação com o GovBr

Embora utilizado uma referência já validada para orientar nosso processo de integração, cada aplicação tem suas peculiaridades e desafios únicos. Portanto, foi necessário não apenas seguir as diretrizes da referência, mas também adaptá-las às especificidades do nosso sistema, garantindo uma integração bem-sucedida que atendesse às nossas necessidades específicas, já que um dos principais desafios adicionais foi a necessidade de acesso a portas externas que o GovBr libera-se o acesso.

### 5.5.3 Gerenciamento de Permissões no Chaincode

No desenvolvimento do chaincode, um aspecto que poderia ser melhorado é o gerenciamento de permissões, especialmente para funções críticas como a criação das badges. Isso exigiria uma abordagem mais refinada para garantir que apenas usuários autorizados pudessem executar certas operações.



#### 5.5.4 Comunicação entre API e Aplicativo

A comunicação entre a API e o aplicativo representou um desafio significativo neste projeto. Foi desenvolvido um sistema de rotas e requisições no front-end e uma estrutura correspondente no backend. Apesar dos desafios relacionados ao tempo e à complexidade técnica, consegui superar essas barreiras e estabelecer uma comunicação efetiva entre os dois componentes.

Por meio de um processo iterativo de desenvolvimento e testes, foi identificado e corrigido erros de código, o que permitiu validar a integração entre a API e o aplicativo. Esta etapa foi crucial para assegurar a funcionalidade do sistema como um todo. Embora foi enfrentado limitações de tempo, que restringiram a amplitude dos testes e ajustes, a comunicação essencial entre a API e o aplicativo foi estabelecida com sucesso.

#### 5.5.5 Integração com Blockchain Pública

A integração com uma blockchain pública não foi alcançada dentro do cronograma deste projeto. As complexidades inerentes ao desenvolvimento e os desafios enfrentados nas fases iniciais consumiram uma parcela significativa do tempo disponível. Consequentemente, a integração com blockchains públicas permanece como um objetivo a ser explorado em trabalhos futuros. Esta etapa é crucial para ampliar a aplicabilidade e a interoperabilidade do sistema em um ambiente mais amplo e diversificado.

## 6 CONCLUSÃO

À medida que este estudo se encerra, é imperativo realizar uma introspecção sobre as jornadas empreendidas, os desafios superados e os sucessos alcançados. Este projeto, focado na implementação de *badges* como mecanismos de gamificação no ensino superior através da tokenização, representou uma incursão significativa nos domínios da tecnologia e da educação.

O objetivo primordial era desenvolver um sistema que utilizasse a tecnologia blockchain para a emissão e administração de *badges* digitais, promovendo a gamificação no contexto acadêmico. Este objetivo foi cumprido através da implementação dos artefatos de código que permitem a existência e apresentação de *badges* na blockchain do Jornada do Estudante. Tal funcionalidade contribuirá para a participação dos alunos e a fortalecerá o uso de blockchain na área de educação.

Mesmo que existissem planos para outras funcionalidades, a proposta foi confrontada com desafios intrínsecos. Um dos desafios mais notáveis foi a integração entre o chaincode, elaborado em Go, e o front-end da aplicação. Esta integração exigiu uma compreensão aprofundada das tecnologias envolvidas e de suas potenciais interações. A harmonização entre o backend, operando em uma blockchain, e um front-end acessível demandou diversas iterações e ajustes para assegurar uma experiência de usuário contínua e eficiente. No fim, este desafio foi superado.

Embora o objetivo inicial de transpor *badges* para blockchains públicas e de estabelecer medidas de privacidade não tenham sido concretizados dentro do prazo deste estudo, devido às complexidades técnicas e logísticas, tal limitação sinaliza direções para pesquisas futuras e desenvolvimentos subsequentes. Esses desafios ainda representam um campo fértil e pouco explorado no trabalho, com potencial para revolucionar o reconhecimento e a partilha de realizações acadêmicas. Isso vale para todos os outros desafios citados na Seção 5.5.

Concluindo, este trabalho constitui um marco relevante na interseção da tecnologia blockchain com o setor educacional. Apesar de nem todos os objetivos terem sido integralmente alcançados, as fundações estabelecidas servirão como base para futuras investigações e inovações. A gamificação no ensino superior, sustentada pela tecnologia blockchain, tem o potencial de transformar a maneira como os estudantes interagem com o seu processo educativo, tornando-o mais cativante, interativo e efetivo.

## REFERÊNCIAS

ARCHANA PRASHANTH JOSHI MENG HAN, Yan Wang. survey on security and privacy issues of blockchain technology. v. 1, p. 121–147, 2018.

BRASIL, CNN. **Gamificação na educação: entenda o que é, importância e como pode ser usada.** [S.l.: s.n.]. Disponível em: <https://www.cnnbrasil.com.br/estilo/gamificacao-na-educacao/>. Acesso em: 2023.

BRASILEIRO, Governo. Padrão Digital de Governo, 2023.

CHIH-HUNG WU, Chien-Yu Liu. Educational Applications of Non-Fungible Token (NFT), 2023.

E-ESTONIA. **Notícia.** [S.l.]. Disponível em: <https://e-estonia.com/solutions/e-identity/id-card/>. Acesso em: 2018.

ELIAS, Bruno Daniel. Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino, 2023.

FERRETTI, Stefano; D'ANGELO, Gabriele. On the Ethereum blockchain structure: A complex networks theory perspective. **Concurrency and Computation: Practice and Experience**, v. 32, ago. 2019.

HONG, Sangwon; NOH, Yoongdo; HWANG, Jeyoung; PARK, Chanik. FabAsset: Unique Digital Asset Management System for Hyperledger Fabric, p. 1269–1274, 2020.

HYPERLEDGER. **Documentação.** [S.l.]. Disponível em: <https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatis.html#>. Acesso em: 19 jun. 2023.

IBM. **O que é Hyper Ledger Fabric?** [S.l.]. Disponível em: <https://www.ibm.com/br-pt/topics/hyperledger>. Acesso em: 1 nov. 2022.

LIN, Shijie. Proof of Work vs. Proof of Stake in Cryptocurrency. **Highlights in Science, Engineering and Technology**, v. 39, p. 953–961, 2023.

MEC. **Site.** [S.l.]. Disponível em: <https://www.gov.br/mec/pt-br/jornadadoestudante>.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**.

[*S.l.: s.n.*], 2008.

NIKOLIĆ, Sara; MATIĆ, Sasa; ČAPKO, Darko; VUKMIROVIĆ, Srđan; NEDIĆ, Nemanja. Development of a Blockchain-Based Application for Digital Certificates in Education, p. 1–4, 2022.

NOTÍCIA. **Site**. [*S.l.*]. Disponível em: <https://www.infomoney.com.br/mercados/o-que-e-a-hyperledger-besu-a-tecnologia-escolhida-para-o-piloto-do-real-digital>.

PALMA, Lucas M.; VIGIL, Martín A. G.; PEREIRA, Fernando L.; MARTINA, Jean E. Blockchain and smart contracts for higher education registry in Brazil. **International Journal of Network Management**, v. 29, n. 3, e2061, 2019. e2061 nem.2061. eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/nem.2061>.

REGISTRY, The Swedish Land. **Noticia**. [*S.l.*]. Disponível em: <https://www.coindesk.com/markets/2018/06/15/swedens-land-registry-demos-live-transaction-on-a-blockchain/>. Acesso em: 15 jun. 2018.

ROBIN WIERUCH. **The Road to React: Your journey to master plain yet pragmatic React.js**. [*S.l.: s.n.*], 2017.

SALEH, Omar S.; GHAZALI, Osman; IDRIS, Norbik Bashah. A New Decentralized Certification Verification Privacy Control Protocol, p. 1–6, 2021.

SETORES. **Noticia**. [*S.l.*]. Disponível em: <https://fargotech.com.br/2021/06/07/blockchain-aplicacoes-2/>. Acesso em: 2021.

SIAL, Muhammad Fateh Khan. Blockchain Technology – Prospects, Challenges and Opportunities. **IEEE Blockchain Technical Briefs**, 2019.

SZABO, Nick. **Artigo**. [*S.l.*]. Disponível em: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>. Acesso em: 1994.

TOLE SUTIKNO, Asa Ismia Bunga Aisyahrani. Non-fungible tokens, decentralized autonomous organizations, Web 3.0, and the metaverse in education: From university to metaversity, 2023.

TOLE SUTIKNO, Asa Ismia Bunga Aisyahrani. Smart contracts on the blockchain - A bibliometric analysis and review Author links open overlay panel, 2021.

WANG, Qin; LI, Rujia; WANG, Qi; CHEN, Shiping. Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges, mai. 2021.

ZHAO, Wenbing; RONG, Chunming; WU, Jun; SUN, Zhixin; SAMPALLI, Srinivas. IEEE Access Special Section Editorial: Blockchain Technology: Principles and Applications. **IEEE Access**, v. 9, p. 110006–110010, 2021.

# Apêndices

## APÊNDICE A – Artigo da monografia

# Badges como ferramenta de gamificação no contexto do ensino superior por meio de tokenização

Brenno Araujo Queiroz <sup>1</sup>

<sup>1</sup>Sistemas de Informação  
Universidade Federal de Santa Catarina (UFSC)

**Abstract.** *The introduction of blockchain technology in education has brought significant benefits, such as the authentication and availability of data related to students' academic trajectories. Tokenization, in particular, offers an additional layer of standardization and facilitates the transfer and sharing of these data, enhancing their utility. However, it is important to recognize that even without tokenization, data stored on the blockchain can be quite useful, thanks to the immutable and transparent nature of the technology. Tokenization is a technique that involves transforming physical or digital assets into tokens, that is, digital units that can be easily stored, transferred, and managed on the blockchain. 'Jornada do Estudante' is a platform that uses blockchain technology to store data related to students' academic trajectories, such as grades, school history, certificates, and other relevant information. The goal of this work is to implement badges corresponding to academic achievements throughout university life. Examples include achievements for the best student in a subject during the semester, best athlete in a sports competition, and top-performing graduate. These badges represent a new feature in the 'Jornada do Estudante' project, using Hyperledger Fabric blockchain to produce Non-Fungible Tokens (NFTs) in an educational context. By facilitating the consumption and storage of these data, as well as providing gamification through the issuance of educational and social badges, these badges are represented in this work as NFTs. A web application was implemented where educational information and achievement badges are displayed, following the 'Jornada do Estudante' standard including the implementation of a chaincode for managing the Badges. Thus, this work contributes to the advancement of blockchain technology in education, through the development of a feature for the 'Jornada do Estudante' platform that allows the issuance of educational badges and encourages student participation.*

**Resumo.** *A introdução da tecnologia blockchain na educação tem trazido benefícios significativos, como a autenticação e a disponibilidade de dados relacionados à trajetória acadêmica dos estudantes. A tokenização, em particular, oferece uma camada adicional de padronização e facilita a transferência e o compartilhamento desses dados, aumentando sua utilidade. No entanto, é importante reconhecer que mesmo sem a tokenização, os dados armazenados na blockchain podem ser bastante úteis, graças à natureza imutável e transparente da tecnologia. A tokenização é uma técnica que consiste em transformar ativos físicos ou digitais em tokens, ou seja, unidades digitais que podem ser facilmente armazenadas, transferidas e gerenciadas na blockchain. O "Jornada do Estudante" é uma plataforma que utiliza a tecnologia blockchain para armazenar os dados relacionados à trajetória acadêmica dos estudantes, como*



*notas, histórico escolar, certificados e outras informações relevantes. O objetivo deste trabalho é implementar badges correspondentes a conquistas acadêmicas ao longo da vida universitária. Exemplos delas são as conquistas de melhor aluno de uma disciplina durante o semestre, melhor atleta de uma competição desportiva e de formando com melhor desempenho. Esses badges representam uma nova funcionalidade no projeto "Jornada do Estudante", utilizando a blockchain Hyperledger Fabric para produzir Non-Fungible Tokens (NFTs) no contexto educacional. Facilitando o consumo e armazenamento desses dados, bem como proporcionando uma gamificação através da emissão de badges educacionais e sociais, esses badges são representados nesse trabalho como NFTs. Foram implementados uma aplicação web onde é exibido informações educacionais e as badges de conquista, seguindo o padrão do "Jornada do Estudante" incluindo a implementação de um chaincode para gerenciamento das Badges. Desta forma, o presente trabalho contribui para o avanço da tecnologia blockchain na educação, através do desenvolvimento de uma funcionalidade para a plataforma "Jornada do Estudante" que permite emissão de badges educacionais e incentiva a participação dos estudantes.*

## **1. Introdução**

No dia 31 de outubro de 2008, uma figura, anônima até então, alteraria definitivamente o curso da história da computação distribuída. No whitepaper "Bitcoin: A Peer-to-peer Electronic Cash System" (NAKAMOTO, 2008), Satoshi Nakamoto estabeleceu os alicerces do que se conhece hoje como criptomoeda e blockchain. O autor anônimo criou uma criptomoeda conhecida como Bitcoin, uma moeda digital representada uma cadeia de assinaturas digitais e evidências criptográficas transmitidos a outros por meio de uma rede peer-to-peer descentralizada.

A rede blockchain tem potencial significativo para transformar a prestação de serviços governamentais, simplificando a troca de informações e coordenando processos entre diversas agências governamentais. Por exemplo, países como a Suécia estão explorando essa tecnologia para agilizar seus registros de propriedades, diminuindo o risco de fraudes e tornando as transferências mais eficientes (REGISTRY, 2018). Além disso, a Estônia tem utilizado a blockchain para estabelecer sistemas de identidade digital, permitindo uma validação de identidade online rápida e segura (E-ESTONIA, 2018).

Desta forma, o Ministério da Educação (MEC) viu o uso de blockchain como oportunidade de aperfeiçoar a rede de ensino, deixando-a segura e rápida. Considerando problemas no sistema de instituições de ensino, os autores (PALMA et al., 2019) propuseram um novo modelo de blockchain e smart contracts nas instituições de ensino superior, onde seria possível guardar dados do processo de formação de maneira transparente e segura. O MEC apreciou esta proposta e iniciou o projeto com o Laboratório de Segurança em Computação (LABSEC) da Universidade Federal de Santa Catarina (UFSC). Entretanto, esse modelo não abrange a parte de tokenization na rede, a qual transformaria os badges dos usuários da Jornada do Estudante em Token.

Este vigente trabalho tem como finalidade realizar a criação de estruturas para permitir a emissão desses badges, que é apresentado ou exibido para indicar alguma realização, além da estrutura, o presente trabalho busca criar um processo de gameificação

para o estudante, visando criar um módulo desta solução dentro do "Jornada do Estudante"(MEC, s.d.). Isso possibilitará que todas as conquistas acadêmicas e extracurriculares sejam tokenizáveis e lastreáveis na rede, ampliando o seu uso.

## 2. Fundamentação teórica

Este capítulo introduz ao leitor os conceitos necessários para entender como funcionam as tecnologias relacionadas a este trabalho e os motivos de serem utilizadas.

### 2.1. Blockchain

A Blockchain é uma tecnologia disruptiva para a construção de consenso e confiança em uma rede peer-to-peer sem controle centralizado. Foi usada pela primeira vez no Bitcoin, a primeira criptomoeda lançada no início de 2009, para implementar um livro razão seguro de transações. A imutabilidade do livro razão (ledger), que corresponde a uma lista encadeada de blocos (ver Figura 1), é uma característica fundamental para assegurar a integridade das transações em uma moeda digital. Ela garante que, após uma transação ser registrada, não possa ser facilmente alterada. No entanto, essa imutabilidade por si só não resolve o desafio do gasto duplo. O gasto duplo refere-se à tentativa de usar a mesma moeda digital em mais de uma transação. Para combater isso, criptomoedas como o Bitcoin empregam mecanismos de consenso, como a prova de trabalho (Proof of Work - PoW). Esse mecanismo valida e confirma transações, tornando extremamente desafiador gastar a mesma moeda duas vezes. Portanto, enquanto a imutabilidade protege a integridade das transações, é o mecanismo de consenso que previne efetivamente o gasto duplo. (ZHAO et al., 2021). Após um período de tranquilidade, o interesse pela blockchain explodiu nos últimos anos. O número de publicações indexadas pela Web of Science sobre blockchain aumentou de 2 em 2013 (o primeiro ano em que publicações sobre blockchain começaram a aparecer), para 4 em 2014, 21 em 2015, 118 em 2016, 521 em 2017 e 1.080 em 2018 (ZHAO et al.,2021).

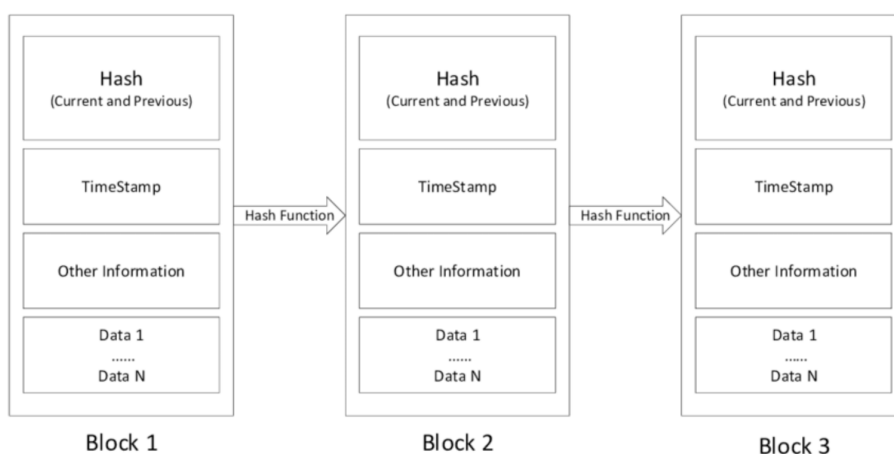


Figure 1. Lista encadeada de blocos

### 2.2. Hyperledger Fabric

O Hyperledger Fabric é uma plataforma de Tecnologia de ledger distribuído (TLD) de nível empresarial, autorizada, e um produto de destaque no panorama da tecnologia de

cadeias de blocos. Foi concebida para suportar implementações de diferentes componentes e acomodar as complexidades existentes no ecossistema económico. É sustentada por uma arquitetura modular que proporciona elevados graus de confidencialidade, resiliência, flexibilidade e escalabilidade.

Esta plataforma é conhecida pela sua utilização em contextos empresariais (NOTÍCIA, s.d.) isso incluindo bancos, finanças, seguros, assistência médica, recursos humanos, cadeia de suprimentos e até distribuição de música digital e oferece capacidades diferenciadoras essenciais em relação a outras plataformas populares de livro-razão distribuído ou de cadeias de blocos.

A Hyperledger Foundation, um esforço de colaboração de código aberto criado para fazer avançar as tecnologias de cadeia de blocos entre sectores, é a força motriz por detrás do Hyperledger Fabric. Acolhida pela Linux Foundation, reúne líderes em domínios como as finanças, a banca, a Internet das Coisas, a cadeia de abastecimento, o fabrico e a tecnologia. A Hyperledger Foundation acolhe uma série de projectos de software de cadeia de blocos de nível empresarial, sendo o Hyperledger Fabric um dos mais proeminentes.

Estes projectos são concebidos e construídos por uma comunidade de programadores diversificada e servem uma vasta gama de partes interessadas, incluindo fornecedores, organizações de utilizadores finais, prestadores de serviços, empresas em fase de arranque, académicos e muito mais. O objetivo é fornecer as ferramentas necessárias para construir e implementar redes de cadeias de blocos ou soluções comerciais. Os colaboradores da Hyperledger Foundation, como parte da equipe mais vasta da Linux Foundation, possui anos de experiência na prestação de serviços de gestão de programas para projectos de código aberto (HYPERLEDGER, 2023).

### **2.3. Ferramentas de Desenvolvimento**

As ferramentas de desenvolvimento desempenham um papel crucial na criação e implementação de soluções baseadas em blockchain. No contexto do Hyperledger Fabric, existem várias ferramentas e linguagens que são comumente usadas.

**Linguagens de Chaincode:** O Chaincode é o termo usado pelo Hyperledger Fabric para se referir aos contratos inteligentes que são executados na blockchain. As linguagens de programação suportadas para escrever chaincodes incluem Go, JavaScript e TypeScript. Cada uma dessas linguagens tem suas próprias vantagens e desvantagens, e a escolha da linguagem de programação pode depender de vários fatores, como a complexidade do contrato inteligente, as habilidades da equipe de desenvolvimento e as necessidades específicas do projeto.

**SDKs/Gateways:** As Software Development Kits (SDKs) e os gateways fornecem uma interface para interagir com a rede blockchain. Eles permitem que os desenvolvedores criem e gerenciem transações, interajam com contratos inteligentes e realizem outras tarefas relacionadas à blockchain. O Hyperledger Fabric suporta SDKs para várias linguagens de programação, incluindo Node.js, Java e Go.

**Hyperledger Caliper:** O Hyperledger Caliper é uma ferramenta de benchmarking que permite aos usuários medir o desempenho de uma blockchain específica sob várias cargas de trabalho. Caliper suporta várias plataformas blockchain, incluindo Hyperledger

Fabric, e pode ser uma ferramenta valiosa para testar e otimizar o desempenho de uma solução blockchain.

Essas ferramentas e linguagens de programação formam a base para o desenvolvimento de aplicações robustas e eficientes na blockchain Hyperledger Fabric. A escolha das ferramentas certas pode ter um impacto significativo na qualidade e eficácia da solução final.

## **2.4. Ethereum e Smart Contracts**

Ethereum é uma plataforma de software baseada em blockchain que permite a construção e execução de contratos inteligentes e as chamadas Aplicações Distribuídas (DApps). Essa plataforma também é a base para uma moeda virtual relacionada, chamada Ether. Para a definição de contratos inteligentes, o Ethereum fornece uma linguagem de programação Turing completa que permite criar programas e executá-los no blockchain (FERRETTI; D'ANGELO, 2019).

Os smart contracts, ou contratos inteligentes, são scripts que estão ancorados em uma blockchain ou infraestrutura distribuída semelhante. Quando acionados por uma transação na blockchain e validados em toda a rede, ações predefinidas são executadas. Dado que as condições de um smart contract são armazenadas de forma transparente na blockchain, ele sempre operará conforme todas as partes pretendem, o que pode reduzir questões de confiança entre as partes envolvidas. Esses contratos são, em essência, scripts de software, semelhantes aos scripts que são executados em aplicações que não são baseadas em blockchain.

O conceito e a ideia subjacente dos smart contracts precedem a emergência do Bitcoin e da tecnologia blockchain. (SZABO, 1994) definiu um smart contract como um protocolo de transação informatizado que atende a condições contratuais, como termos de pagamento, confidencialidade ou execução, reduzindo exceções e minimizando a necessidade de intermediários confiáveis. Ele citou protocolos de dinheiro digital como exemplos de smart contracts, pois esses mecanismos permitem pagamentos online combinados com características de dinheiro em papel, como divisibilidade e confidencialidade.

No entanto, é importante notar que tanto o termo "smart" quanto "contract" podem ser enganosos. Um smart contract consiste em um código de computador simples e raramente representa um constructo legalmente vinculativo. Buterin, o fundador da Ethereum, expressou arrependimento por adotar o termo "smart contracts", sugerindo que deveria ter escolhido um nome mais técnico e menos sugestivo (TOLE SUTIKNO, 2021).

Um exemplo simples de um smart contract é um sistema automatizado de gerenciamento de quartos de hotel. Assim que um cliente deixa o quarto, o smart contract é automaticamente notificado. Por exemplo, um dispositivo conectado à porta do quarto atua como um oráculo que inicia transações na blockchain sempre que a porta é usada. Isso, por sua vez, aciona processos predefinidos, como faturamento ou atribuição automática de pessoal de limpeza.

No caso da Ethereum, os smart contracts são escritos em uma linguagem de programação Turing completa chamada Solidity. A linguagem é compilada em bytecode e executada na máquina virtual Ethereum (EVM). Transações assinadas por chaves privadas podem invocar a execução de funções de um smart contract. Pode-se ver um exemplo de

smart contract em Solidity na Figura 2, o qual possui uma função que retorna o saldo do contrato em Eth, criptomoeda da Ethereum.

A tecnologia blockchain, que permite a transferência segura de valor peer-to-peer (p2p) pela internet entre partes que não confiam mutuamente, ofereceu pela primeira vez uma infraestrutura distribuída adequada para a aplicação de smart contracts. Uma vez que os termos predefinidos são cumpridos, a blockchain executa transparentemente o código, e nenhuma entidade externa pode interferir (TOLE SUTIKNO, 2021).

```
1 // Código exemplo de um Smart Contract
2
3 pragma solidity ^0.8.0;
4
5 contract Balance {
6     function balance() public returns (uint256){
7         return payable(address(this)).balance;
8     }
9 }
```

**Figure 2. Código exemplo de um Smart Contract**

## 2.5. NON-FUNGIBLE TOKEN (NFT)

Os NFT são um tipo de criptomoeda que é derivada dos contratos inteligentes do Ethereum. O NFT foi proposto pela primeira vez nas Propostas de Melhoria do Ethereum (EIP)-721 e posteriormente desenvolvido no EIP-1155(WANG et al., 2021). Os NFTs diferem das criptomoedas clássicas, como o Bitcoin, em suas características intrínsecas. O Bitcoin é uma moeda padrão na qual todas as moedas são equivalentes e indistinguíveis. Em contraste, o NFTs é único e não pode ser trocado como se fosse igual (ou seja, não fungível), tornando-o adequado para identificar algo ou alguém de maneira única (WANG et al., 2021). Os NFTs têm atraído notável atenção tanto da comunidade industrial quanto científica. Foi relatado que o volume médio de negociação de 24 horas do mercado de NFTs é de 4,592,146,914 USD, enquanto o volume de negociação de 24 horas de todo o mercado de criptomoedas é de 341,017,001,809 USD (WANG et al., 2021). A liquidez das soluções relacionadas ao NFT representou 1,3% de todo o mercado de criptomoedas em um curto período (5 meses)(WANG et al., 2021).

## 3. Trabalhos Correlatos

A tecnologia de NFTs na blockchain da hyperledger ainda é muito nova e isto ficou evidente durante a realização da revisão bibliográfica sistemática. Quando fala-se de Badges na hyperledger tomando como premissa que é derivado da tecnologia de NFT e junto a isso o benefício de aplicar essa tecnologia no sistema educacional pela Fabric, são poucos os artigos que abordam esta temática de forma completa, por estes motivos optou-se por analisar artigos que abordassem cada uma das temáticas de forma separada, representando o real estado da arte.

Ao todo, foram produzidos resumos de cinco trabalhos, incluindo "A New Decentralized Certification Verification Privacy Control Protocol"(SALEH; GHAZALI; IDRIS, 2021), "Educational Applications of Non-Fungible Token (NFT)"(CHIH-HUNG WU, 2023), "Development of a Blockchain-Based Application for Digital Certificates

in Education”(NIKOLIĆ et al., 2022), ”Non-fungible tokens, decentralized autonomous organizations, Web 3.0, and the metaverse in education: From university to metaversity”(TOLE SUTIKNO, 2023), e ”FabAsset: Unique Digital Asset Management System for Hyperledger Fabric”(HONG et al., 2020). Esses trabalhos foram peças centrais para a produção deste trabalho.

### **3.1. A New Decentralized Certification Verification Privacy Control Protocol**

Este artigo, intitulado ”A New Decentralized Certification Verification Privacy Control Protocol”, foi escrito por Omar S. Saleh, Osman Ghazali e Norbik Bashah Idris. O estudo discute o uso da tecnologia blockchain na verificação de certificados acadêmicos e propõe um novo protocolo descentralizado de controle de privacidade para verificação de certificados.

Os certificados acadêmicos são uma convenção social que oferece um meio de atestar novos conhecimentos obtidos por uma pessoa ou entidade sobre uma pessoa ou entidade. A falsificação de certificados é uma prática comum que prejudica o investimento e a confiança nos sistemas de ensino superior. A blockchain foi introduzida para melhorar o processo de verificação de certificados acadêmicos e surgiu como uma maneira potencial de autenticar documentos e como uma ferramenta eficaz para combater fraudes e uso indevido de documentos.

No entanto, a preservação da privacidade foi um desafio na maioria das soluções existentes. A privacidade indica que o certificado protege tanto a identidade quanto as informações. Portanto, é proposto um novo protocolo de controle de privacidade descentralizado para verificação de certificação. O protocolo proposto pode ser usado para emissão e verificação de certificados educacionais, mantendo a privacidade e a confidencialidade tanto no nível de rede (nível de ministérios, universidades e estudantes) quanto no nível de dados.

A solução descentralizada foi implementada usando Hyperledger Fabric como infraestrutura e Javascript como linguagem de contrato. As características da blockchain, como imutabilidade, transparência e confiabilidade, são valiosas não apenas em criptomoedas, mas também em vários outros campos, levando ao desenvolvimento de aplicações baseadas em blockchain em áreas como governo, educação, saúde e ciência.

A pesquisa estabeleceu e abordou o valor da tecnologia blockchain na autenticação de certificados educacionais, bem como as complexidades de sua implementação na educação. Um dos principais problemas identificados no processo de verificação de certificados baseado em blockchain é a proteção da privacidade. A privacidade e a confidencialidade garantem que a identidade e as informações presentes no certificado estejam seguras. Portanto, foi proposto um novo Protocolo Descentralizado de Controle de Privacidade para Verificação de Credenciais.

O protocolo proposto visa proteger a privacidade e a confidencialidade no nível da rede, envolvendo ministérios, universidades e estudantes. O protocolo será introduzido e implementado em instituições educacionais selecionadas para trabalhos futuros.

### **3.2. Educational Applications of Non-Fungible Token (NFT)**

O artigo ”Educational Applications of Non-Fungible Token (NFT)”, escrito por Chih-Hung Wu e Chien-Yu Liu, explora o potencial das aplicações educacionais de NFTs no

setor de educação. Com a emergência dos NFTs na tecnologia blockchain, as instituições de ensino podem utilizar NFTs para recompensar os alunos por meio do processamento automático de informações de transações e processos de compra e venda de material escolar usando a tecnologia de contratos inteligentes. Isso permite o estabelecimento de níveis de reconhecimento e incentiva os alunos a receberem recompensas de reconhecimento em NFT.

De acordo com a Pirâmide de Aprendizado Taxonômica, o aprendizado através de experiências práticas desempenha um papel crucial na atração do interesse dos alunos. Neste estudo, os autores analisam o potencial do uso de NFTs na educação e as aplicações atuais dos NFTs na sociedade. Eles conduzem um estudo de caso e realizam uma investigação preliminar dos tipos de aplicações NFT na indústria educacional. Em seguida, analisam diferentes setores educacionais usando análise individual combinada com análise SWOT para entender o impacto, o valor e os desafios das aplicações de NFT.

Os resultados revelam 10 aplicações educacionais de NFTs: livros didáticos; microcertificados; históricos escolares e registros; bolsas de estudo e direitos; masterclasses e criação de conteúdo; experiências de aprendizado; registro e coleta de dados; patentes, inovação e pesquisa; arte; pagamento e depósito. Por fim, o artigo discute maneiras de reduzir o impacto negativo dos NFTs educacionais no ambiente sustentável.

### **3.3. Development of a Blockchain-Based Application for Digital Certificates in Education**

O artigo "Development of a Blockchain-Based Application for Digital Certificates in Education" discute a criação de um sistema de gerenciamento escolar baseado em blockchain conhecido como "Eternal Digital Certificate". Este sistema tem como objetivo principal armazenar informações sobre eventos escolares e seus participantes, além de emitir certificados para esses eventos.

A plataforma blockchain escolhida para armazenar essas informações é a Polygon Supernets, que é uma rede descentralizada de blockchains. Os certificados são emitidos como NFTs para os estudantes que completaram com sucesso todos os cursos de um evento e são mantidos em suas carteiras pessoais. Esses certificados não podem ser vendidos ou transferidos para outra carteira.

O uso de um sistema blockchain para armazenar informações de educação e carreira de uma pessoa simplifica o processo de análise de dados, tornando-se útil na avaliação de candidatos a empregos, bolsas e outras situações que exijam a classificação de pessoas com base em critérios que incluem o nível de educação. Além disso, como o sistema é descentralizado, não há necessidade de terceiros para verificar os certificados. Isso pode ser especialmente útil para estudantes que se transferirem de uma instituição para outra, pois facilita o processo de verificação e equivalência de disciplinas.

### **3.4. Non-fungible tokens, decentralized autonomous organizations, Web 3.0, and the metaverse in education: From university to metaversity**

O artigo "Non-fungible tokens, decentralized autonomous organizations, Web 3.0, and the metaverse in education: From university to metaversity" discute o impacto das tecnologias NFTs, DAOs, Web 3.0 e metaverso na educação. O blockchain permite a utilização de

NFTs para validar diplomas universitários e históricos escolares, e as DAOs estão sendo implementadas para automatizar e autenticar cursos e certificados.

A Web 3.0 é uma evolução da internet que torna-a legível por máquinas, enquanto o metaverso oferece experiências imersivas e interativas aos alunos. A "metaversidade" é uma referência a um campus virtual que fornece uma experiência de metaverso para a educação, permitindo que os alunos participem de aulas e atividades educacionais em realidade virtual.

### **3.5. FabAsset: Unique Digital Asset Management System for Hyperledger Fabric**

O artigo "FabAsset: Unique Digital Asset Management System for Hyperledger Fabric", escrito por Sangwon Hong, Yoongdoo Noh, Jeyoung Hwang e Chanik Park, aborda o gerenciamento de ativos digitais únicos na plataforma de blockchain permissionada Hyperledger Fabric.

O artigo identifica a necessidade de suporte a NFTs na plataforma, visto que a versão 2.0.0 alpha do Hyperledger Fabric introduziu o FabToken, que suporta apenas tokens fungíveis (FTs). Para abordar essa lacuna, os autores apresentam o FabAsset, um sistema de gerenciamento de ativos digitais únicos para o Hyperledger Fabric. O FabAsset avança o XNFT (modelo extensível de NFT para Fabric), modularizando seus componentes em chaincode (ou seja, contrato inteligente para o Fabric) e SDK para construir um sistema completo para NFTs.

Os autores também demonstram um protótipo de serviço de assinatura descentralizado para validar a utilidade do FabAsset. O objetivo do artigo é aproveitar o potencial dos NFTs no contexto das blockchains empresariais e expandir as capacidades do Hyperledger Fabric para incluir o suporte a esses ativos digitais únicos.

## **4. Proposta**

Este capítulo destina-se a discutir a proposta central deste TCC, que é a implementação de uma nova funcionalidade no projeto "Jornada do Estudante". A funcionalidade proposta é a tokenização, ou seja, a utilização da blockchain Hyperledger para produzir NFTs representando badges no contexto educacional.

A inspiração para esta proposta vem, inicialmente, do trabalho correlato "FabAsset: Unique Digital Asset Management System for Hyperledger Fabric" (HONG et al., 2020). Este trabalho demonstra um protótipo que aproveita o potencial dos NFTs no contexto das blockchains empresariais, expandindo as capacidades do Hyperledger Fabric para incluir o suporte a esses ativos digitais únicos.

Além disso, uma inspiração significativa para a implementação do front-end e do processo de autenticação veio do TCC de Bruno Daniel Elias, "Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino" (ELIAS, 2023). O trabalho de Elias fornece um modelo valioso para a integração segura e eficiente de sistemas de autenticação, utilizando o acesso do gov.br, que é fundamental para a gestão de identidades digitais no contexto da nossa proposta.

Neste capítulo, exploraremos como essas capacidades podem ser utilizadas para realmente produzir esses ativos no contexto do projeto "Jornada do Estudante". Discutiremos os detalhes da implementação, os desafios esperados e os resultados potenciais desta



proposta. A abordagem integrada, combinando as inovações do FabAsset com as práticas de autenticação e segurança de dados do trabalho de Elias, oferece uma base sólida para o desenvolvimento de um sistema robusto e eficaz no contexto educacional.

## **5. Implementação**

A implementação desta proposta é um processo que envolve duas vertentes principais: o desenvolvimento de chaincodes e a criação de uma interface gráfica. Ambos são fundamentais para o sucesso do projeto, cada um desempenhando um papel único e complementar.

**Desenvolvimento de Chaincodes:** Os chaincodes, que são os contratos inteligentes na blockchain Hyperledger Fabric, formam a base do nosso sistema. Eles são projetados para definir as regras de criação, emissão e transferência de badges. Esses contratos garantem que todas as transações sejam realizadas conforme as normas estabelecidas, assegurando a autenticidade e a imutabilidade das badges. O desenvolvimento desses chaincodes exige proficiência na linguagem de programação Go, uma escolha popular para escrever chaincodes para a Hyperledger Fabric.

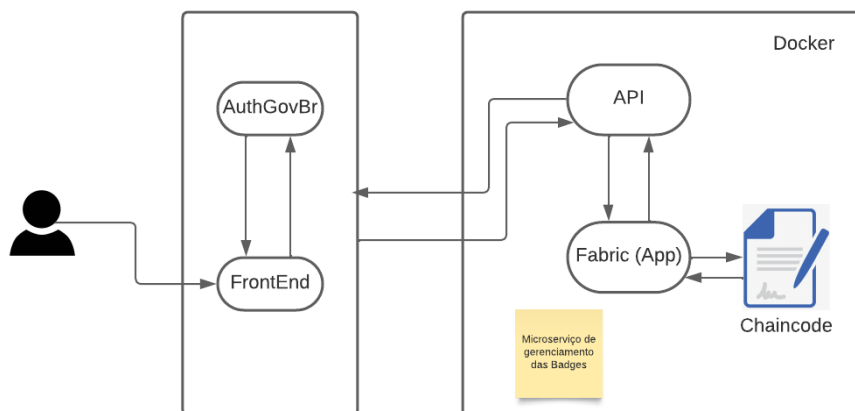
**Criação da Interface Gráfica:** Paralelamente, a interface gráfica representa o ponto de contato entre os usuários (estudantes e instituições de ensino) e a blockchain. Esta interface é projetada para ser intuitiva e amigável, permitindo que os usuários visualizem facilmente seus dados na blockchain, incluindo as badges. A acessibilidade é uma prioridade, garantindo que a interface possa ser utilizada eficazmente por todos, independentemente do seu nível de conhecimento técnico. Para o desenvolvimento desta interface, utilizaremos a SDK do Node para Hyperledger Fabric, que oferece ferramentas para facilitar a interação com a blockchain.

Portanto, a implementação desta proposta envolverá tanto o desenvolvimento de chaincodes quanto a criação de uma interface gráfica. Ambos os componentes serão desenvolvidos em paralelo, para garantir que funcionem de forma integrada e proporcionem uma experiência de usuário suave e eficaz. No desenvolvimento deste projeto, adotamos um modelo arquitetônico e funcional, ilustrado na Figura 3, que serve como a espinha dorsal do nosso sistema. A arquitetura do modelo é composta por vários componentes chave, cada um desempenhando um papel vital no funcionamento geral do sistema:

Temos o usuário, que se conecta com o front-end e que faz requisição para se autenticar com o GovBr, o qual habilita credenciais para o acesso desse usuário ao sistema. Ao acessar o front autenticado o sistema se comunica com a Application Programming Interface (API) que fornece acesso aos métodos providos pelas aplicações, e essa API se comunica com a aplicação APP permitindo uma integração eficiente e uma comunicação fluida entre diferentes partes do sistema. APP, implementada a partir do SDK do Node para Hyperledger Fabric, faz requisições ao chaincode para recuperar badges criadas. Esse conjunto de quatro serviços é comumente utilizado para outras chaincodes no projeto Jornada do Estudante.

### **5.1. Contribuições da Proposta**

A proposta apresentada neste trabalho traz várias contribuições significativas, tanto para o projeto Jornada do Estudante quanto para o campo mais amplo da educação e da tecnologia blockchain. Entre elas estão:



**Figure 3. Modelo Proposto**

1. **Incentivo à Participação dos Alunos:** Ao implementar badges como NFT para reconhecer e recompensar as conquistas dos alunos, esperamos incentivar a participação ativa dos alunos. Isso pode se manifestar de várias maneiras, desde o aumento do envolvimento nas atividades acadêmicas e esportivas até a melhoria do desempenho acadêmico. Além disso, ao registrar as *soft skills* dos alunos, como liderança, trabalho em equipe e resolução de problemas, podemos ajudar a destacar essas habilidades importantes que muitas vezes são subestimadas no ambiente acadêmico tradicional.
2. **Contribuição para o Projeto Jornada do Estudante:** A implementação de NFT no projeto Jornada do Estudante representa uma inovação significativa. Ao aproveitar a tecnologia blockchain, podemos melhorar a segurança, a transparência e a verificabilidade das conquistas dos alunos. Isso pode aumentar a confiança no projeto Jornada do Estudante e melhorar sua eficácia como uma ferramenta para apoiar o desenvolvimento dos alunos.
3. **Avanço da Tecnologia Blockchain na Educação:** Ao implementar NFT no contexto educacional, estamos explorando novas maneiras de aplicar a tecnologia blockchain na educação. Isso pode abrir caminho para futuras inovações e contribuir para o desenvolvimento da tecnologia blockchain como uma ferramenta valiosa para melhorar a educação.

## 6. Protótipo

Neste capítulo, detalharemos o protótipo desenvolvido para a implementação de badges digitais como ferramentas de gamificação no ensino superior, empregando a tecnologia blockchain Hyperledger Fabric. Este protótipo, uma extensão inovadora do projeto "Jornada do Estudante", foca na criação e gerenciamento de NFTs que representam as conquistas educacionais dos alunos.

O desenvolvimento deste protótipo foi realizado com uma abordagem integrada, combinando tecnologias de front-end modernas com processos de chaincode robustos na blockchain Hyperledger. A chaincode, crucial para o funcionamento da nossa solução blockchain, foi escrita em Go. Esta linguagem foi escolhida por sua eficiência e adequação ao desenvolvimento de chaincodes, permitindo-nos definir regras de negócio

precisas e lógica de transação para os NFTs. Essa implementação assegura operações seguras e confiáveis na blockchain, essenciais para a emissão e gerenciamento das badges digitais.

Para a infraestrutura, utilizamos servidores virtuais, otimizando a conectividade e interação com a blockchain. A interface do usuário foi desenvolvida com tecnologias atuais, como React.js, para garantir uma experiência de usuário intuitiva e envolvente.

Um aspecto fundamental deste protótipo é a integração com o sistema de autenticação do gov.br, inspirado pelo trabalho de Bruno Daniel Elias em seu TCC "Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino"(ELIAS, 2023). Implementamos uma API de autenticação customizada, utilizando o Login Único do gov.br, para autenticar os usuários de forma segura e vincular suas identidades digitais aos registros na blockchain.

Neste capítulo, além de apresentar a configuração da rede Hyperledger e a implementação da chaincode em Go, também discutiremos a arquitetura e o fluxo de trabalho do sistema. Para uma compreensão visual, incluímos um fluxograma do front-end (ver Figura 4) e do chaincode (ver Figura 5), que ilustra o processo de interação entre as diferentes componentes do sistema, desde a autenticação do usuário até a emissão e gerenciamento das badges digitais. Discutiremos os desafios técnicos, as soluções adotadas e as inovações implementadas, destacando a importância da chaincode e a influência do trabalho de Bruno Daniel Elias no desenvolvimento do nosso sistema de autenticação.

Finalizaremos com uma discussão sobre os resultados esperados deste protótipo, ressaltando seu potencial para aumentar o engajamento dos alunos e enriquecer o processo educacional através da gamificação e da tecnologia blockchain.

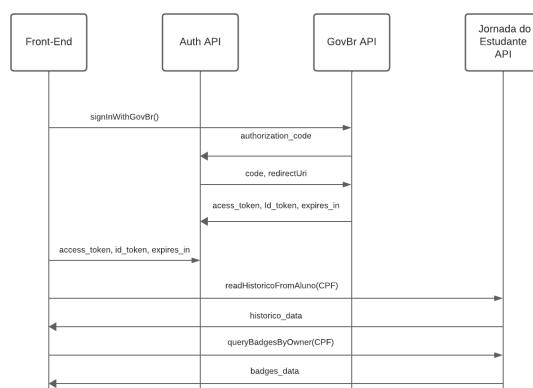


Figure 4. Fluxograma Front-end

## 6.1. Chaincode

No desenvolvimento do chaincode do prototipo em Go, foi projetado para o gerenciamento de badges no formato de NFTs na plataforma Hyperledger Fabric. O chaincode é uma peça central no sistema de blockchain, responsável por definir as regras de negócio e a lógica de manipulação dos dados. Neste caso, o foco é na criação, transferência, revogação e consulta de badges, que representam conquistas ou credenciais digitais.

### 6.1.1. Estrutura do Chaincode

O chaincode é estruturado em torno de várias componentes principais:

- Definição da Estrutura Badge A estrutura Badge é definida para representar um NFT. Ela inclui campos como Owner, TokenType, TokenName, Description, BasicDescription, IpfsImage, IssuerCpf, IssueDate e ExtraAttributes, que armazenam informações relevantes sobre cada badge.
- SmartContract Struct A estrutura SmartContract serve como a espinha dorsal do chaincode, dentro da qual todas as funções operacionais são definidas.
- Funções de Inicialização e Invocação As funções Init e Invoke são implementadas para atender aos requisitos do Hyperledger Fabric. Init é usada para qualquer inicialização necessária durante a instanciação do chaincode, enquanto Invoke roteia as chamadas para diferentes funções com base no nome da função fornecido.

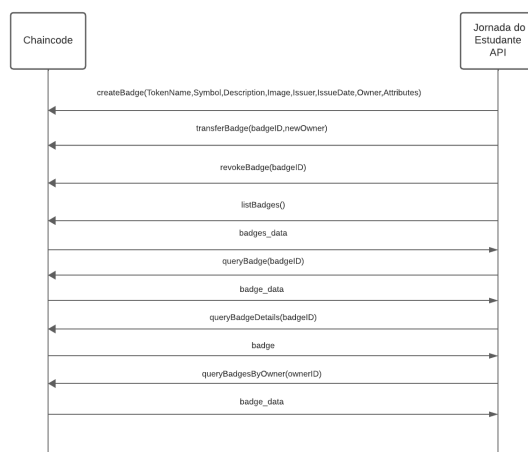


Figure 5. Fluxograma Chaincode Badge

## 6.2. Front-End

No desenvolvimento do front-end do nosso protótipo, focamos em proporcionar uma experiência de usuário intuitiva e agradável, essencial para a interação eficaz com o sistema. O design foi elaborado seguindo as diretrizes do Design System GovBr (BRASIL, 2023). Nosso objetivo era criar uma interface responsiva e de fácil navegação, com uma estética moderna que atendesse às expectativas e necessidades dos usuários contemporâneos.

Para alcançar esse objetivo, escolhemos utilizar tecnologias modernas e amplamente adotadas no desenvolvimento do front-end. React.js foi a escolha principal devido à sua flexibilidade, eficiência e o suporte de uma ampla comunidade. Esta tecnologia nos permitiu criar uma interface dinâmica e reativa, que responde de maneira fluida às interações dos usuários. Além disso, a integração de frameworks e bibliotecas adicionais, como Styled-Components para o layout e Axios para as requisições HTTP, foi crucial para a eficiência do desenvolvimento e a robustez do sistema. Styled-Components facilitou a criação de um layout consistente e responsivo, enquanto Axios aprimorou a gestão das comunicações de rede, assegurando uma interação suave com o back-end.

Combinando essas tecnologias, conseguimos desenvolver um front-end que não só é visualmente atraente, mas também funcional e fácil de usar. Acreditamos que esta

abordagem não apenas melhora a experiência do usuário, mas também desempenha um papel vital na aceitação e satisfação do usuário, fatores cruciais para o sucesso de qualquer aplicação digital no ambiente educacional atual.

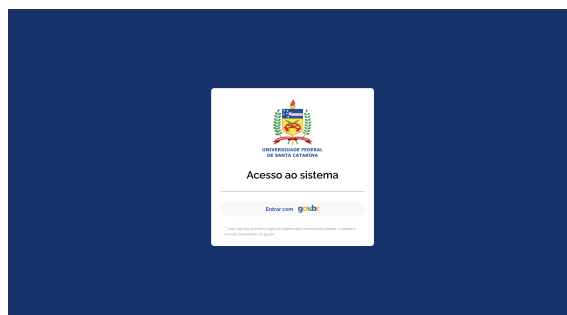


Figure 6. Página de Login

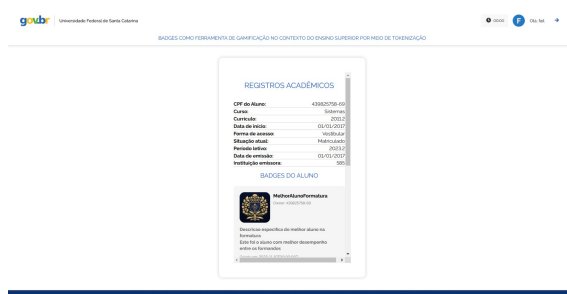


Figure 7. Página de Home

## 7. Conclusão

À medida que este estudo se encerra, é imperativo realizar uma introspecção sobre as jornadas empreendidas, os desafios superados e os sucessos alcançados. Este projeto, focado na implementação de badges como mecanismos de gamificação no ensino superior através da tokenização, representou uma incursão significativa nos domínios da tecnologia e da educação.

O objetivo primordial era desenvolver um sistema que utilizasse a tecnologia block- chain para a emissão e administração de badges digitais, promovendo a gamificação no contexto acadêmico. Este objetivo foi cumprido através da implementação dos artefatos de código que permitem a existência e apresentação de badges na blockchain do Jornada do Estudante. Tal funcionalidade contribuirá para a participação dos alunos e a fortalecerá o uso de blockchain na área de educação.

Mesmo que existissem planos para outras funcionalidades, a proposta foi confrontada com desafios intrínsecos. Um dos desafios mais notáveis foi a integração entre o chaincode, elaborado em Go, e o front-end da aplicação. Esta integração exigiu uma compreensão aprofundada das tecnologias envolvidas e de suas potenciais interações. A harmonização entre o backend, operando em uma blockchain, e um front-end acessível demandou diversas iterações e ajustes para assegurar uma experiência de usuário contínua e eficiente. No fim, este desafio foi superado.

Embora o objetivo inicial de transpor badges para blockchains públicas e de estabelecer medidas de privacidade não tenham sido concretizados dentro do prazo deste estudo, devido às complexidades técnicas e logísticas, tal limitação sinaliza direções para pesquisas futuras e desenvolvimentos subsequentes. Esses desafios ainda representam um campo fértil e pouco explorado no trabalho, com potencial para revolucionar o reconhecimento e a partilha de realizações acadêmicas.

Concluindo, este trabalho constitui um marco relevante na interseção da tecnologia blockchain com o setor educacional. Apesar de nem todos os objetivos terem sido integralmente alcançados, as fundações estabelecidas servirão como base para futuras investigações e inovações. A gamificação no ensino superior, sustentada pela tecnologia blockchain, tem o potencial de transformar a maneira como os estudantes interagem com o seu processo educativo, tornando-o mais cativante, interativo e efetivo.

## 8. Referências

As referências utilizadas neste presente artigo se refere:

[Nakamoto 2008], [Lucas M. Palma 2019], [IBM a], [Zhao et al. 2021], [Sial 2019], [Wöhrrer and Zdun 2018], [Nikolić et al. 2022], [e Estonia ], [Chih-Hung Wu 2023], [Hong et al. 2020], [Ferretti and D’Angelo 2019], [Brasil ], [brasileiro 2023], [IBM b], [Hyperledger ], [MEC ], [Lin 2023], [Archana Prashanth Joshi 2018], [Saleh et al. 2021], [Wang et al. 2021], [Tole Sutikno 2023], [Szabo ], [Notícia ], [Palma et al. 2019], [Robin Wieruch 2017], [Setores ], [Tole Sutikno 2021], [Teixeira 2015], [Elias 2023] e [Registry ]

## References

- Archana Prashanth Joshi, Meng Han, Y. W. (2018). survey on security and privacy issues of blockchain technology. 1:121–147.
- Brasil, C. Gamificação na educação: entenda o que é, importância e como pode ser usada. brasileiro, G. (2023). Padrão digital de governo.
- Chih-Hung Wu, C.-Y. L. (2023). Educational applications of non-fungible token (nft). e Estonia. *Noticia*.
- Elias, B. D. (2023). Identificação e autenticação de estudantes em uma rede blockchain de ensino.
- Ferretti, S. and D’Angelo, G. (2019). On the ethereum blockchain structure: A complex networks theory perspective. *Concurrency and Computation: Practice and Experience*, 32.
- Hong, S., Noh, Y., Hwang, J., and Park, C. (2020). Fabasset: Unique digital asset management system for hyperledger fabric. pages 1269–1274.
- Hyperledger. *Documentação*.
- IBM. *O que é a tecnologia blockchain?*
- IBM. *O que é Hyper Ledger Fabric?*

- Lin, S. (2023). Proof of work vs. proof of stake in cryptocurrency. *Highlights in Science, Engineering and Technology*, 39:953–961.
- Lucas M. Palma, Martín A. G. Vigil, F. L. P. J. E. M. (2019). *Blockchain and smart contracts for higher education registry in Brazil*.  
MEC. *Site*.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- Nikolić, S., Matić, S., Čapko, D., Vukmirović, S., and Nedić, N. (2022). Development of a blockchain-based application for digital certificates in education. pages 1–4.  
Notícia. *Site*.
- Palma, L. M., Vigil, M. A. G., Pereira, F. L., and Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in brazil. *International Journal of Network Management*, 29(3):e2061. e2061 nem.2061.
- Registry, T. S. L. *Noticia*.
- Robin Wieruch (2017). *The Road to React: Your journey to master plain yet pragmatic React.js*.
- Saleh, O. S., Ghazali, O., and Idris, N. B. (2021). A new decentralized certification verification privacy control protocol. pages 1–6.  
Setores. *Noticia*.
- Sial, M. F. K. (2019). Blockchain technology – prospects, challenges and opportunities. *IEEE Blockchain Technical Briefs*.
- Szabo, N. *Artigo*.
- Teixeira, F. (2015). *O que é SUS ?*
- Tole Sutikno, A. I. B. A. (2021). Smart contracts on the blockchain - a bibliometric analysis and review author links open overlay panel.
- Tole Sutikno, A. I. B. A. (2023). Non-fungible tokens, decentralized autonomous organizations, web 3.0, and the metaverse in education: From university to metaversity.
- Wang, Q., Li, R., Wang, Q., and Chen, S. (2021). Non-fungible token (nft): Overview, evaluation, opportunities and challenges.
- Wöhler, M. and Zdun, U. (2018). Design patterns for smart contracts in the ethereum ecosystem. pages 1513–1520.
- Zhao, W., Rong, C., Wu, J., Sun, Z., and Sampalli, S. (2021). Ieee access special section editorial: Blockchain technology: Principles and applications. *IEEE Access*, 9:110006–110010.