UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

GABRIEL ROCHA ALVES DA SILVA

SISTEMA DE GERENCIAMENTO DE CREDENCIAIS PARA UNIVERSITÁRIOS BASEADO EM BLOCKCHAIN

FORTALEZA

2024

GABRIEL ROCHA ALVES DA SILVA

SISTEMA DE GERENCIAMENTO DE CREDENCIAIS PARA UNIVERSITÁRIOS BASEADO EM BLOCKCHAIN

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Orientador: Prof. Dr. Paulo A. L. Rego

Coorientador: Prof. Me. Maurício M. Neto

FORTALEZA

2024

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

S58s Silva, Gabriel Rocha Alves da.
Sistema de gerenciamento de credenciais para universitários baseado em blockchain / Gabriel Rocha Alves da Silva. – 2024.
45 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Centro de Tecnologia, Curso de Engenharia de Computação, Fortaleza, 2024.
Orientação: Prof. Dr. Paulo Antonio Leal Rego.
Coorientação: Prof. Me. Maurício M. Neto.

1. Blockchain. 2. Etherium. 3. Solana. 4. Credenciamento estudantil. I. Título.

CDD 621.39

GABRIEL ROCHA ALVES DA SILVA

SISTEMA DE GERENCIAMENTO DE CREDENCIAIS PARA UNIVERSITÁRIOS BASEADO EM BLOCKCHAIN

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Paulo A. L. Rego (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Me. Maurício M. Neto (Coorientador)
Universidade Federal do Ceará (UFC)

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

AGRADECIMENTOS

Aos meus pais, Francisco José e Eliziane Rocha, pelo amor incondicional e apoio constante ao longo desta jornada.

Ao meu irmão, Rafael Rocha, pelo incentivo e companheirismo.

Ao meu orientador, Prof. Paulo Rego, pela orientação experiente e dedicação ao meu desenvolvimento acadêmico.

Ao meu coorientador, Prof. Me. Maurício M. Neto, pela colaboração valiosa e contribuições significativas para o aprimoramento deste trabalho.

À minha namorada, Aila Beatriz, pela amizade e apoio, que foram fundamentais para a conclusão deste projeto.

RESUMO

A gestão e autenticação de certificados acadêmicos enfrentam diversos desafios com os métodos tradicionais, incluindo a dependência de terceiros para acesso, vulnerabilidades de armazenamento e processos lentos de verificação. Além disso, a falta de informações detalhadas nos certificados e o impacto significativo das fraudes, destacam a necessidade de uma solução mais robusta e segura.

Este trabalho desenvolve uma aplicação baseada em tecnologia blockchain para enfrentar esses desafios. A proposta visa desenvolver uma aplicação para gerenciar e autenticar certificados acadêmicos utilizando a tecnologia blockchain. Foram estabelecidos objetivos específicos, como criar um sistema robusto contra falsificações, facilitar um processo de validação ágil e confiável, e avaliar as blockchains Ethereum e Solana para a implementação de contratos inteligentes. A aplicação desenvolvida, utilizando Ethereum e Solana, demonstrou eficácia na emissão e verificação digital dos certificados, com Solana oferecendo custos de transação significativamente menores. Os resultados evidenciam que a solução é segura, transparente e eficiente para a gestão de certificados acadêmicos.

Palavras-chave: Blockchain, Etherium, Solana, Credenciamento Estudantil

ABSTRACT

Challenges in the management and authentication of academic certificates with traditional methods include dependence on third parties for access, storage vulnerabilities, and slow verification processes. Additionally, the lack of detailed information on certificates and the significant impact of fraud highlight the need for a more robust and secure solution.

This work develops an application based on blockchain technology to address these challenges. The proposal aims to develop an application for managing and authenticating academic certificates using blockchain technology. Specific objectives were established, such as creating a system robust against forgeries, facilitating an agile and reliable validation process, and evaluating the Ethereum and Solana blockchains for implementing smart contracts. The developed application, using Ethereum and Solana, demonstrated effectiveness in the digital issuance and verification of certificates, with Solana offering significantly lower transaction costs. The results show that the solution is secure, transparent, and efficient for the management of academic certificates.

Keywords: Blockchain. Ethereum. Solana. Student Credentialing

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Os certificados estudantis desempenham um papel fundamental como testemunhos escritos que validam competências, formação, presença e colaboração da comunidade acadêmica. Esses certificados podem ser emitidos de diversas formas, cada uma com métodos específicos de verificação e validação:

- **Certificados Físicos:** Tradicionalmente, são emitidos em papel, com elementos de segurança como hologramas, marcas d'água, e assinaturas físicas. A verificação normalmente envolve contato direto com a instituição emissora para validar a autenticidade do documento.
- **Certificados Digitais:** São emitidos em formato eletrônico, na maior parte dos casos assinados digitalmente para garantir sua autenticidade. A validação pode ser feita por meio de sistemas online que conferem a assinatura digital e outros elementos de segurança digital, como códigos QR.
- **Open Badges:** Um formato padrão para credenciais digitais que representam conquistas, habilidades ou competências. Eles contêm metadados verificáveis, como emissor, critérios de obtenção e data de emissão, que podem ser validados através de plataformas compatíveis.

No entanto, cada tipo de certificado apresenta seus próprios desafios:

- **Acesso Dependente de Terceiros (Certificados Físicos e Digitais):** Em modelos tradicionais, seja em papel ou formato eletrônico, os estudantes muitas vezes não têm acesso direto às suas próprias credenciais, dependendo de terceiros para fornecer cópias.
- **Vulnerabilidade de Armazenamento (Certificados Físicos e Digitais):** Se as organizações ou indivíduos responsáveis pelo armazenamento das credenciais interromperem esse serviço, os certificados podem se tornar inválidos ou inacessíveis.
- **Verificação Lenta (Certificados Físicos):** O processo de verificação de certificados tradicionais em papel é frequentemente demorado, podendo levar semanas após a solicitação (JIRGENSONS; KAPENIEKS, 2018a).
- **Limitações dos Certificados Educacionais (Certificados Físicos, Digitais e Open Badges):** Determinados elementos essenciais podem estar ausentes, tais como descrições das habilidades adquiridas, níveis de domínio alcançados e atividades extracurriculares (trabalhos voluntários, estágios, intercâmbio, etc). Os fatores pessoais, como criatividade, motivação ou potencial de liderança, também não são abordados, mesmo que possam

oferecer uma visão mais completa das conquistas e potencial dos alunos (JIRGENSONS; KAPENIEKS, 2018b).

Além dessas questões, é importante abordar o impacto das fraudes relacionadas a certificados, especialmente aqueles emitidos fisicamente. Em janeiro de 2005, dois especialistas na área chamaram o negócio de diplomas falsos de "indústria de bilhões de dólares que vendeu mais de um milhão de diplomas universitários falsos" (EZELL; BEAR, 2005). Diante desses desafios, torna-se evidente a necessidade de um sistema que ofereça certificados à prova de violação, de fácil acesso e verificação rápida.

A Blockchain, conhecida por sua estrutura descentralizada e imutável, oferece uma solução segura e transparente para a gestão de certificados digitais. Sua capacidade de registrar transações de forma distribuída, sem a necessidade de intermediários, garante a autenticidade e a integridade dos documentos emitidos. Além disso, a natureza descentralizada da blockchain reduz o risco de fraudes e falsificações, tornando-a uma ferramenta ideal para o gerenciamento de credenciais acadêmicas (TAPSCOTT; TAPSCOTT, 2016).

A motivação para este trabalho surge da crescente demanda por soluções tecnológicas que solucionem os desafios na emissão e verificação de certificados acadêmicos. A tecnologia Blockchain se destaca como uma alternativa promissora para resolver esse problema. O público-alvo do projeto inclui instituições de ensino superior, órgãos certificadores, e estudantes que necessitam de uma forma confiável de emissão e verificação de seus certificados acadêmicos.

1.1 Objetivos Geral e Específicos

O presente trabalho tem por objetivo geral desenvolver uma aplicação capaz de gerenciar e autenticar certificados utilizando a tecnologia blockchain, explorando a eficácia deste modelo em superar desafios associados ao ciclo de vida dos certificados digitais.

No projeto, a escolha das plataformas Ethereum e Solana é justificada por suas características complementares. O Ethereum, amplamente utilizado e consolidado no mercado, é a plataforma de contratos inteligentes mais relevante e madura, com uma vasta comunidade de desenvolvedores, o que facilita a integração e oferece maior segurança devido à sua ampla adoção. Por outro lado, Solana surge como uma alternativa mais acessível, com taxas de transação significativamente mais baixas e alta escalabilidade, tornando-a ideal para aplicações que demandam baixo custo e alta velocidade.

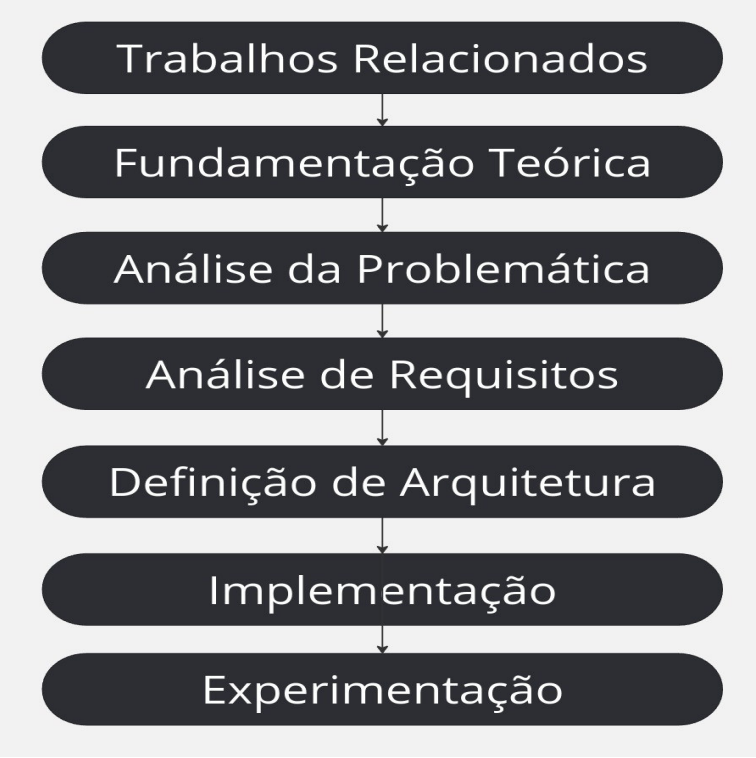
O estudo apresenta os seguintes objetivos específicos:

1. Pesquisar e analisar diferentes soluções de blockchain aplicáveis ao gerenciamento de certificados digitais.
2. Planejar e implementar uma ferramenta que gerencie credenciais e integre com as blockchains Solana e Ethereum.
3. Avaliar a solução desenvolvida, realizando comparações entre as blockchains Solana e Ethereum.

1.2 Metodologia

Para o desenvolvimento deste trabalho de conclusão de curso, a metodologia apresentada na Figura 1 foi utilizada.

Figura 1 – Ilustração representativa do ciclo da Metodologia



Fonte: Elaborado pelos autores

Trabalhos Relacionados: A metodologia empregada neste trabalho começou com estudo de casos de sucesso de plataformas que utilizam blockchain para gerenciamento de credenciais. Esses estudos de caso forneceram informações valiosos sobre a implementação e operação de sistemas de certificação baseados em blockchain. A análise de casos reais permite validar as abordagens teóricas com práticas comprovadas no mercado.

Fundamentação Teórica: Foi feita a revisão da literatura específica sobre o tema da pesquisa.

Esta revisão focou nos conceitos fundamentais da blockchain e nas técnicas utilizadas em plataformas de gerenciamento de credenciais. A revisão de literatura é crucial para compreender e identificar lacunas que a pesquisa pretende preencher.

Análise da Problemática: A análise da problemática envolve a identificação e compreensão dos desafios enfrentados no gerenciamento de credenciais tradicionais. Esta etapa foca na definição clara dos problemas que a pesquisa busca resolver. Identificar a problemática é essencial para direcionar a pesquisa de forma objetiva e relevante.

Análise de Requisitos: A análise de requisitos consiste na identificação das necessidades funcionais e não funcionais que o sistema deve atender. Este processo é fundamental para garantir que o sistema desenvolvido atenda às expectativas e demandas dos usuários. A definição clara dos requisitos orienta o desenvolvimento e a validação do sistema.

Definição de Arquitetura: A definição de arquitetura detalha a estrutura técnica e os componentes principais do sistema proposto. Esta etapa abrange a seleção das tecnologias e protocolos a serem utilizados. A arquitetura bem definida é crucial para garantir a escalabilidade, segurança e eficiência do sistema.

Implementação: A implementação envolve a construção do sistema conforme a arquitetura definida. Esta etapa inclui o desenvolvimento de código, integração de componentes, e configuração de infraestrutura. A implementação é essencial para transformar os requisitos e a arquitetura em um sistema funcional.

Experimentação: A experimentação foi conduzida para avaliar o desempenho e a eficácia do sistema desenvolvido. Esta etapa incluiu a definição do cenário de teste, métricas utilizadas para avaliação, ameaças à validade dos resultados, e o período de realização dos testes. A análise dos resultados obtidos durante os experimentos forneceu dados importantes para a conclusão da pesquisa e sugestões para trabalhos futuros.

1.3 Estrutura do Trabalho

Este trabalho está organizado da seguinte forma:

Capítulo 2: Trabalhos Relacionados

Analisa trabalhos anteriores sobre o mesmo tema ou temas semelhantes, destacando as abordagens utilizadas e os resultados obtidos.

Capítulo 3: Fundamentação Teórica

Apresenta os conceitos fundamentais sobre certificação digital, blockchain e estudos

anteriores relacionados ao uso dessas tecnologias no contexto educacional.

Capítulo 4: Desenvolvimento da Aplicação

Detalha o processo de desenvolvimento da aplicação de gerenciamento e autenticação de certificados, com ênfase na implementação da tecnologia blockchain.

Capítulo 5: Experimentação e Discussões

Apresenta os resultados obtidos com a aplicação desenvolvida e discute sua eficácia em relação aos objetivos propostos.

Capítulo 6: Conclusão

Resume as principais conclusões do trabalho, destacando as contribuições, limitações e sugestões para trabalhos futuros.

2 TRABALHOS RELACIONADOS

A literatura possui diversas soluções que têm sido propostas e desenvolvidas com o intuito de empregar a tecnologia blockchain no campo da educação. Neste contexto, nossa discussão se restringe aos sistemas e arquiteturas que enfatizam a verificação baseada em blockchain e a distribuição de certificados acadêmicos.

O país de Malta tornou-se a primeira nação a adotar a tecnologia blockchain na educação, emitindo diplomas digitais, certificados de treinamento e declarações de equivalência, fazendo uso do padrão BlockCerts (HOLOTESCU, 2018). O BlockCerts é uma plataforma de código aberto atualmente desenvolvido pelo Instituto de Tecnologia de Massachusetts (MIT) e concentra-se principalmente na emissão e verificação de certificados oficiais por meio da blockchain (OLIVER *et al.*, 2018). O BlockCerts é fundamentado no conceito de identidade auto-soberana de todos os participantes, oferecendo componentes para criar, emitir, visualizar e verificar certificados.

O EduCTX (TRUKANOVIC *et al.*, 2018) propôs um sistema unificado global para créditos e classificação de ensino superior, baseado no Sistema Europeu de Transferência e Acumulação de Créditos (ECTS), no qual moedas são transferidas para a blockchain a fim de representar os créditos acadêmicos obtidos pelos estudantes. Esse modelo requer que tanto os estudantes quanto os verificadores mantenham credenciais criptográficas ou identidades digitais para participar do ecossistema.

O UZHBC é um sistema de verificação baseado em blockchain, desenvolvido especificamente para diplomas emitidos pela Universidade de Zurique (GRESCH *et al.*, 2018). Esse sistema faz uso da blockchain pública Ethereum e emprega um contrato inteligente tanto para a emissão quanto para a verificação, aceitando um PDF do documento como entrada. Notavelmente, esse sistema não inclui um órgão de acreditação.

Por outro lado, a Universidade de Nicósia, no Chipre, também está adotando a tecnologia blockchain para registrar as conquistas dos alunos (University of Nicosia,). A UNIC utiliza a blockchain do Bitcoin para diversas atividades, como pagamentos de taxas e emissão de certificados acadêmicos por meio dessa tecnologia, desde 2017. Para preservar a autenticidade dos certificados, utiliza o algoritmo de hash SHA-256. Contudo, a UNIC ainda carece de um método claro para autenticar as partes envolvidas e apresenta requisitos insuficientes para que um empregador verifique o certificado.

Em (TARIQ *et al.*, 2019), os autores propuseram um sistema de acreditação e

verificação de diplomas baseado em blockchain, denominado Cerberus. Esse sistema utilizava contratos inteligentes on-chain para revogação de credenciais e não exige que estudantes ou empregadores gerenciar identidades digitais ou credenciais criptográficas para utilizar o sistema.

2.1 Discussão

A Tabela 1 apresenta uma comparação entre diferentes sistemas de certificação baseados em blockchain.

Tabela 1 – Comparação de Sistemas de Certificação Baseados em Blockchain

Sistema	**BlockCerts**	**EduCTX**	**UZHBC**	**UNIC**	**Cerberus**
Desenvolvedor	MIT	Trabalho Acadêmico	Universidade de Zurique	Universidade de Nicósia	Trabalho Acadêmico
Base de Tecnologia	Ethereum/BitCoin	Hyperledger	Ethereum	Bitcoin	Proprietária
Foco Principal	Emissão e Verificação de Certificados	Global Higher Education Credit Platform	Verificação de Diplomas	Emissão de Certificados	Mitigação de Fraudes de Credenciais
Identidade Digital	Sim	Sim	Não	Não	Não
Órgão de Acreditação	Sim	Não	Sim	Sim	Não
Contratos Inteligentes	Sim	Não	Sim	Não	Sim
Gestão de Identidade	Sim	Não	Não	Não	Não

Fonte: Adaptado do autor.

Os critérios selecionados para a comparação dos sistemas de certificação baseados em blockchain foram escolhidos para fornecer uma análise abrangente e relevante das capacidades e características de cada sistema. Esses critérios incluem:

- **Sistema** O nome do sistema de certificação baseado em blockchain, que representa a solução ou plataforma em questão. Este critério ajuda a identificar e comparar diferentes abordagens e soluções disponíveis para certificação digital.
- **Desenvolvedor** Refere-se à entidade ou grupo responsável pelo desenvolvimento do sistema.
- **Base de Tecnologia** Indica a plataforma blockchain utilizada pelo sistema.
- **Foco Principal** Descreve o objetivo principal do sistema, como a emissão e verificação de certificados, a gestão de créditos acadêmicos, ou a mitigação de fraudes de credenciais.
- **Identidade Digital** Indica se o sistema suporta a criação e o gerenciamento de identidades digitais. A identidade digital é fundamental para garantir a autenticidade dos indivíduos

envolvidos e a integridade dos dados de certificação.

- **Órgão de Acreditação** Refere-se se o sistema possui uma entidade de acreditação oficial que valida e endossa os certificados emitidos.
- **Contratos Inteligentes** Especifica se o sistema utiliza contratos inteligentes para automatizar processos e garantir a execução das regras definidas.
- **Gestão de Identidade** Indica se o sistema oferece funcionalidades para a gestão de identidades dos participantes, além da simples verificação.

O projeto desenvolvido propõe o uso da tecnologia blockchain, especificamente através das redes Ethereum e Solana, para a gestão de contratos inteligentes. Essa escolha tecnológica visa aproveitar as características distintas de cada rede para otimizar a implementação e a gestão de credenciais, com um foco especial na eficiência de custos. A análise comparativa entre essas plataformas constitui um aspecto central do projeto, buscando identificar as abordagens mais econômicas sem comprometer a segurança ou a funcionalidade.

Além disso, o projeto tem como objetivo utilizar mecanismos de identidade digital e gestão de identidade. Essa funcionalidade é fundamental para garantir a autenticidade e a integridade dos participantes e dos certificados emitidos, estabelecendo uma camada adicional de confiança e segurança no sistema.

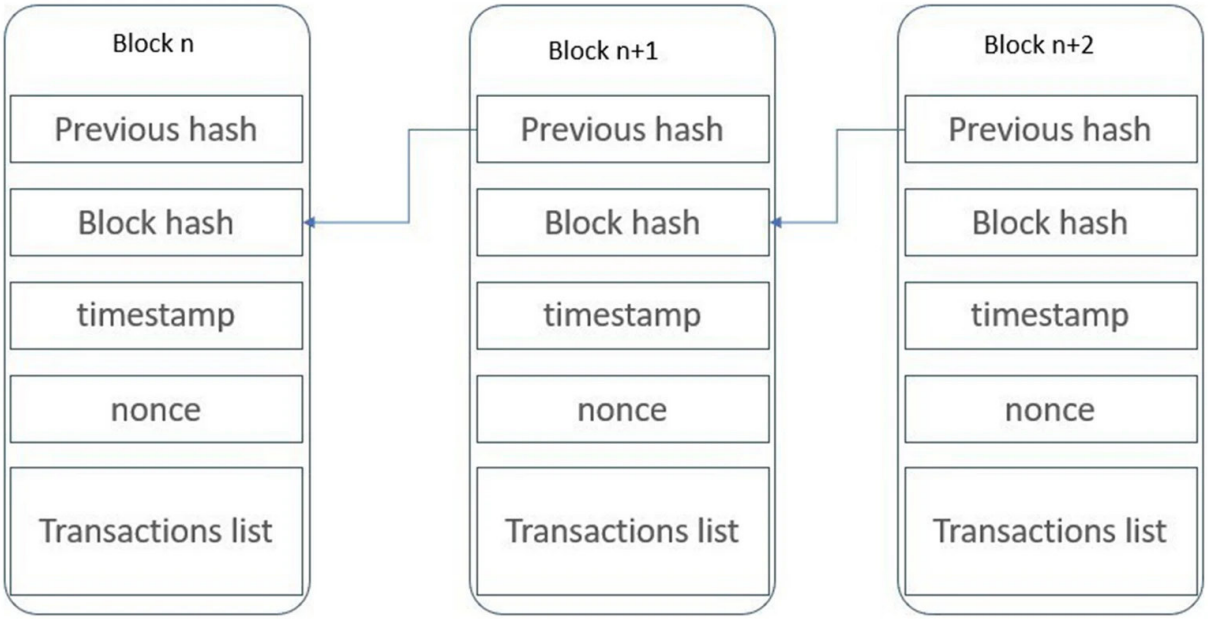
3 FUNDAMENTAÇÃO TEÓRICA

3.1 Blockchain e Seus Mecanismos de Consenso

A blockchain é, de maneira resumida, nas palavras de Grech e Camilleri (2017), "um livro-razão distribuído que proporciona uma forma de registrar e compartilhar informações entre uma comunidade". Essa tecnologia ganhou destaque devido à sua capacidade de garantir a integridade e segurança dos registros.

A estrutura da blockchain é singular, os dados das transações são organizados em blocos, que, por sua vez, estão interligados para formar uma cadeia contínua. Cada bloco abriga informações essenciais, incluindo um registro de data e hora, o valor *hash* do bloco anterior, o valor *hash* do bloco atual e os dados pertinentes (LIN; LIAO, 2017). A característica fundamental da blockchain consiste no fato de que qualquer alteração em um bloco da corrente resultaria imediatamente na modificação do valor do seu *hash* correspondente. O valor *hash* é uma sequência de caracteres gerada por uma função de hash que transforma qualquer conjunto de dados em uma saída de comprimento fixo. Qualquer alteração nos dados originais resulta em um valor de hash completamente diferente, o que torna a detecção de alterações muito fácil.

Figura 2 – Ilustração de registros de transações em uma série de blocos, formando uma blockchain



Fonte: Adapting blockchain's proof-of-work mechanism for multiple traveling salesmen problem optimization

Para adicionar um novo bloco à cadeia, a maioria dos nós na rede deve validar tanto o novo bloco quanto as transações contidas nele. Esse processo é conhecido como mecanismo

de consenso (NOFER *et al.*, 2017). Dois mecanismos de consenso predominantes merecem destaque: o *Proof of Work* (Proof of Work) e o *Proof of Stake* (Proof of Stake). O PoW requer que todas as máquinas na blockchain tenham uma cópia do livro-razão e cada uma resolva um quebra-cabeças complexo relacionado à nova versão desse livro. Já o PoS é uma alternativa mais eficiente em termos energéticos, em que a seleção das máquinas é baseada na quantidade de moedas detidas por um minerador (ZHENG *et al.*, 2017).

A blockchain se destaca por suas características de descentralização e imutabilidade. Os mineradores, provenientes de diversos grupos e indivíduos, participam ativamente da validação das transações, garantindo uma rede robusta e distribuída (LIN; LIAO, 2017).

Essas características fazem da blockchain uma solução promissora para a verificação de certificados, uma vez que garante acesso ininterrupto e validação confiável, independentemente de problemas e imprevistos com a instituição emissora ou seus registros. Isso contrasta com sistemas centralizados, onde interrupções podem resultar na perda permanente do acesso a certificados válidos.

3.2 Contratos Inteligentes

Os contratos inteligentes são programas autoexecutáveis que residem em uma blockchain e são acionados automaticamente quando condições pré-determinadas são cumpridas. Eles são escritos em linguagens de programação específicas e imutáveis, garantindo assim que as regras do contrato sejam seguidas exatamente como foram definidas, sem a possibilidade de alteração ou interferência externa.

3.3 Ethereum

A Ethereum, criada por Vitalik Buterin e lançada em 2015, é uma plataforma de código aberto, descentralizada e turing-completa. Ela pode ser considerada como uma espécie de "sistema operacional global" que possibilita a criação de aplicativos descentralizados (comumente conhecidos como *DApps*) e contratos inteligentes (conhecidos como *Smart-Contracts*) (CHENG *et al.*, 2018).

A Ethereum é especialmente notável por sua Máquina Virtual Ethereum (Do inglês, *Ethereum Virtual Machine*, EVM), que é fundamental para a execução de contratos inteligentes. A EVM é uma blockchain programável que permite que os desenvolvedores executem progra-

mas de computador de acordo com suas necessidades específicas (CHENG *et al.*, 2018). Ao contrário do Bitcoin, que oferece um conjunto fixo de funcionalidades, a EVM proporciona aos desenvolvedores a liberdade de criar contratos inteligentes capazes de automatizar a execução de acordos e operações financeiras.

Suas características individuais:

- **Contratos Inteligentes**: Ethereum é pioneira no conceito de contratos inteligentes, permitindo que qualquer transação complexa seja programada e executada automaticamente.
- **Descentralização**: Não há controle central sobre a rede Ethereum, o que garante maior segurança e resistência à censura.
- **Turing Completo**: A EVM suporta uma ampla gama de cálculos, oferecendo uma flexibilidade que outras blockchains como Bitcoin não possuem.

Suas principais vantagens:

- **Ampla Adoção**: Ethereum tem a maior comunidade de desenvolvedores entre as blockchains, facilitando o desenvolvimento de novos aplicativos descentralizados.
- **Interoperabilidade**: A Ethereum permite que diferentes contratos inteligentes e DApps interajam uns com os outros, criando um ecossistema interconectado.
- **Segurança**: A descentralização e os protocolos criptográficos robustos garantem que as operações na rede Ethereum sejam seguras contra ataques e fraudes.

Custos associados:

- **Gás**: O custo das operações na rede Ethereum é medido em gás, e os preços do gás podem variar dependendo da demanda e da complexidade da transação.
- **Custo de Implementação**: Desenvolver e manter contratos inteligentes na Ethereum pode ser caro, especialmente durante períodos de alta demanda, quando os preços do gás aumentam significativamente.

Exemplos de uso:

- **Uniswap**: Uma plataforma de troca descentralizada que permite a negociação direta de criptomoedas sem a necessidade de um intermediário centralizado.
- **Cryptokitties**: Um jogo baseado em blockchain que permite a criação e comercialização de gatos digitais colecionáveis, mostrando o potencial dos NFTs (tokens não fungíveis).

Bibliotecas para Contratos Inteligentes:

- **OpenZeppelin**: Um conjunto de bibliotecas padronizadas que ajudam a criar contratos inteligentes seguros e auditados.
- **Truffle**: Uma suíte de desenvolvimento para Ethereum que oferece ferramentas para a criação, teste e implantação de contratos inteligentes.
- **Web3.js**: Uma biblioteca JavaScript que permite a interação com a blockchain Ethereum de forma fácil e eficiente.

3.4 Solana

Solana é uma plataforma blockchain de alto desempenho projetada para fornecer escalabilidade e segurança para aplicativos descentralizados (DApps) e contratos inteligentes. Lançada em 2020, a Solana se destaca por sua arquitetura única que visa resolver os problemas de escalabilidade enfrentados por outras redes blockchain.

Suas características individuais:

- **Proof of History (PoH)**: Um mecanismo de consenso que cria uma "prova"cronológica do histórico de eventos na blockchain, melhorando a eficiência e a escalabilidade.
- **Tower BFT**: Um sistema de tolerância a falhas bizantinas que aumenta a segurança e confiabilidade da rede, garantindo a resistência a ataques.
- **Escalabilidade**: Capaz de processar milhares de transações por segundo (TPS), superando significativamente outras redes blockchain como Ethereum.

Suas principais vantagens:

- **Alta Velocidade**: A arquitetura de Solana permite transações rápidas e de baixo custo, tornando-a ideal para aplicativos de alta demanda.
- **Baixos Custos de Transação**: As taxas de transação em Solana são significativamente mais baixas do que na Ethereum, permitindo operações mais econômicas.
- **Crescimento Rápido**: A rede Solana tem atraído um grande número de desenvolvedores e projetos devido à sua eficiência e escalabilidade.

Custos associados:

- **Taxas de Transação**: As taxas são pagas em Sol, a criptomoeda nativa da rede Solana, e são geralmente baixas devido à eficiência da rede.
- **Custos de Implementação**: Embora os custos gerais sejam menores que os da Ethereum, a implementação em Solana ainda exige um entendimento técnico robusto da arquitetura PoH.

Exemplos de uso:

- **Serum**: Um protocolo de finanças descentralizadas (DeFi) que oferece troca de criptomoedas em alta velocidade e com baixo custo.
- **Metaplex**: Uma plataforma para a criação, venda e leilão de NFTs na blockchain Solana, demonstrando o potencial da rede em casos de uso de ativos digitais.

Bibliotecas para Contratos Inteligentes:

- **Anchor**: Um framework para o desenvolvimento de programas em Solana, simplificando o processo de criação e implantação de contratos inteligentes.
- **Solana Web3.js**: Uma biblioteca JavaScript que permite a integração com a blockchain Solana e facilita a criação de DApps.
- **Solana SPL**: Um conjunto de bibliotecas padrão da Solana para o desenvolvimento de tokens e outros ativos digitais.

3.5 Transações

Tanto no Ethereum quanto na Solana, o processamento de transações é essencial para o funcionamento seguro e eficiente das redes blockchain. No Ethereum, uma transação refere-se a uma ação iniciada por uma conta gerenciada por uma ação humana, enquanto na Solana, as transações são processadas de forma semelhante. Em ambas as redes, cada ação computacional tem um custo associado, conhecido como Gas no Ethereum e taxas de transação na Solana, onde as taxas de transação são pagas em Sol, a criptomoeda nativa da rede Solana. Essas taxas representam o custo total das operações realizadas em uma transação.

As principais vantagens das transações são:

- **Resistência à Spam**: O uso de taxa impede que atores maliciosos sobrecarreguem a rede com atividades fraudulentas. Esse mecanismo de prevenção é crucial para garantir a integridade da rede e sua capacidade de processar transações legítimas de forma eficaz.
- **Desencorajamento de Transações Caras**: Uma das funções principais das taxas é impor custos às operações de computação na rede. Isso significa que enviar spam para a rede com transações caras, seja por engano ou com intenções maliciosas, se torna financeiramente desencorajado. Esse sistema de taxação contribui para a utilização responsável da rede.
- **Limite de Computação**: As taxas também estabelecem um limite rígido na quantidade de computação que pode ser executada a qualquer momento em ambas as redes. Esse limite ajuda a evitar que a rede fique sobrecarregada, garantindo que ela esteja sempre

acessível e funcional. Isso é particularmente importante em um ambiente onde a demanda por recursos computacionais pode variar amplamente.

4 FERRAMENTA GESTÃO DE CREDENCIAIS UNIVERSITÁRIAS

Neste capítulo, serão apresentados os princípios fundamentais do desenvolvimento da ferramenta. Além disso, será discutido como os diferentes componentes da solução interagem para alcançar os objetivos do projeto, oferecendo uma visão clara e detalhada da estrutura e funcionamento.

4.1 Requisitos Funcionais

Os requisitos funcionais descrevem o comportamento que o sistema deve ter em relação às suas funcionalidades. Eles especificam as ações que o sistema deve ser capaz de realizar para atender às necessidades dos usuários e dos negócios. Em nossa ferramenta, esses requisitos foram discutidos em reuniões entre orientadores e autores, com base também em estudos de casos e pesquisas. Em nosso sistema inclui:

1. Cria, edita ou remove uma credencial e conecta-a à sua rede blockchain.
2. Escolhe entre Solana ou Ethereum como plataforma para criar uma credencial.
3. Cria um evento para gestão de múltiplas credenciais.
4. Função da Instituição:
    - Gerencia e referencia dados divulgados.
    - Usuários podem se associar a cargos em diferentes instituições.
5. O sistema deve contemplar três níveis de acesso: master, administrativo e colaborador.
6. Funções do Usuário nível master:
    - Criar uma instituição.
    - Convidar usuários para fazer parte da instituição.
    - Definir cargos (administrativo ou colaborador) para os integrantes da instituição.
    - Realizar todas as funções permitidas a um usuário administrativo.
7. Todos os usuários que pertencem à instituição podem criar eventos para gerenciar credenciais para a instituição.
8. Funções do Usuário nível administrativo:
    - Gerenciar o fluxo de eventos de uma credencial.
    - Realizar a precificação dos eventos para Solana ou Ethereum.
9. O evento de geração de credenciais deve permitir:
    - Armazenar credenciais para atualização, edição e remoção.

- Validar individualmente os dados de cada credencial do evento.
- Conectar-se à blockchain escolhida e incrementar as credenciais na blockchain.

10. O evento poderá ter os seguintes estados:
    - Em Revisão: Criação de eventos e validação preliminar dos metadados.
    - Aprovado: Administrador verifica e aprova os metadados do evento.
    - Rejeitado: Administrador verifica e rejeita os metadados do evento.
    - Em Execução: Implementação das credenciais nas redes Ethereum ou Solana.
    - Concluído: Operação bem-sucedida e registro imutável na blockchain.
    - Parcialmente Concluído: Algumas credenciais não foram atualizadas com sucesso.
    - Falha: Operação não concluída devido a falhas. Incidente registrado e notificação enviada.
11. Qualquer usuário pode ter acesso à lista de credenciais publicadas por uma instituição.

4.2 Requisitos Não Funcionais

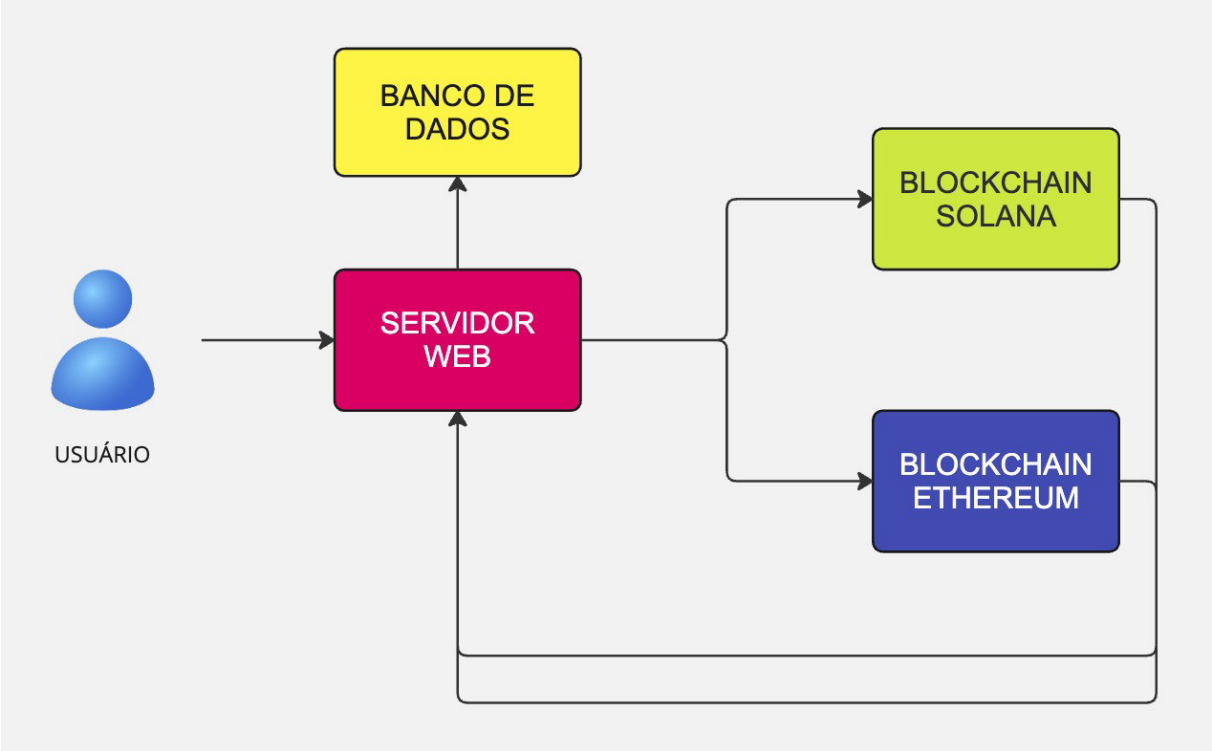
Os requisitos não funcionais descrevem como o sistema deve se comportar em termos de confiabilidade, segurança, escalabilidade, entre outros aspectos.

1. Escalabilidade
    - Expansão de Recursos: A arquitetura do sistema deve permitir a adição de novos módulos ou funcionalidades sem grandes alterações na estrutura existente.
2. Segurança
    - Autenticação e Autorização: Implementar mecanismos de autenticação e autorização para garantir que apenas usuários autorizados acessem e modifiquem informações sensíveis.
3. Manutenibilidade
    - Logs e Monitoramento: Implementar mecanismos de logging detalhado e monitoramento contínuo para facilitar a detecção de problemas e a análise de desempenho.
4. Interoperabilidade
    - Integração com Outras Plataformas: O sistema deve ser capaz de integrar-se facilmente com outras plataformas e serviços externos, utilizando APIs padrão e protocolos comuns (ex.: REST).

4.3 Definição de arquitetura

A Figura 3 ilustra os componentes que formam a estrutura do projeto. A seguir, comentaremos sobre estes:

Figura 3 – Ilustração representativa da arquitetura do sistema



Fonte: Elaborado pelos autores

1. **Servidor Web:**

   Ruby on Rails é um framework de desenvolvimento de aplicações web escrito na linguagem de programação Ruby. Adota uma abordagem de desenvolvimento ágil, enfatizando convenções em vez de configuração (HANSSON, 2008). Entre as principais características, destacam-se: MVC (Model-View-Controller), adoção de convenções sensatas para minimizar a quantidade de configuração necessária (HANSSON, 2008), e promoção da redução da repetição de código, incentivando o uso de abstrações e módulos reutilizáveis (FREEMAN, 2013).

   A arquitetura do Ruby on Rails oferece várias vantagens que se alinham com os requisitos não funcionais do sistema. Em termos de escalabilidade, Rails permite a adição de novos módulos e funcionalidades com modificações mínimas na estrutura existente, facilitando a expansão e adaptação conforme necessário. A segurança é aprimorada com o Rails através da implementação de mecanismos de autenticação e autorização. Para a manutenibilidade,

Rails fornece ferramentas para logging detalhado e monitoramento contínuo, o que facilita a detecção de problemas e a análise de desempenho, alinhando-se às melhores práticas de manutenção. Além disso, a interoperabilidade é suportada pelo Rails por meio de sua compatibilidade com APIs padrão e protocolos comuns, como REST, permitindo uma integração fácil com outras plataformas e serviços externos.

Desenvolvemos, portanto, um monólito em Ruby on Rails para a criação de um serviço web REST, que atua como uma camada intermediária entre os usuários e os contratos inteligentes nas redes Ethereum e Solana. Esta API é responsável por gerenciar todo o fluxo de eventos e operações relacionadas às credenciais, desde a sua criação inicial até a conclusão e publicação dos dados na blockchain.

No exemplo abaixo, temos às informações de um curso de graduação. O objeto inclui detalhes como o nome do curso, o identificador da instituição, o nome do autor e metadados adicionais. A seguir, o código é apresentado para solicitar ao servidor web gere credenciais de um evento:

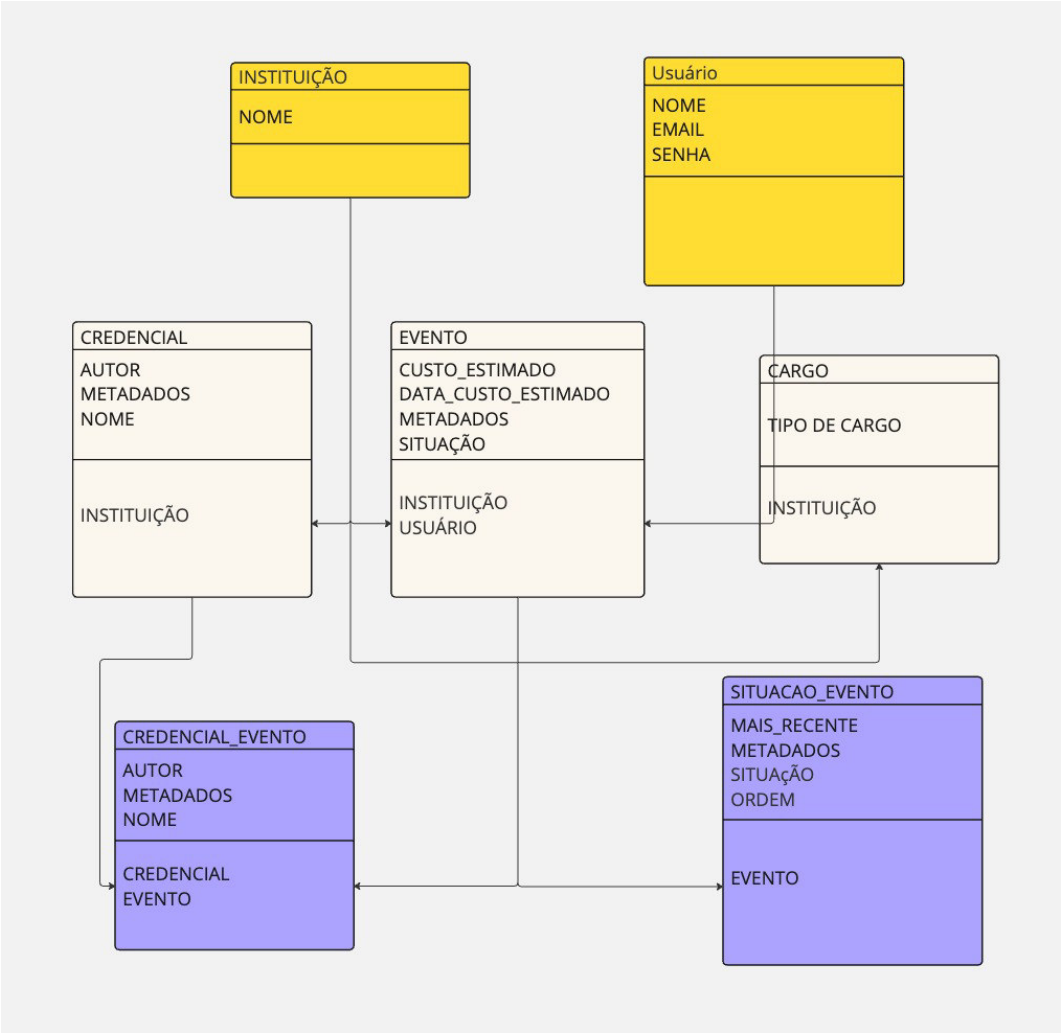
```
{
    evento: {
        "nome": "Graduacao em Engenharia de Computacao",
        "id_insituicao": "1",
    },
    credenciais: [
        {
            "nome": "Graduacao em Engenharia de Computacao",
            "id_insituicao": "1",
            "autor": "Gabriel Rocha",
            "metadados": "{\"curso\": \"Engenharia da
               Computacao\", \"instituicao\": \"Universidade
               Federal do Ceara\", \"duracao\": \"5 anos\",
               \"modalidade\": \"Presencial\", \"ano_inicio
               \": 2020, \"ano_conclusao\": 2025, \"descricao
               \": \"Curso focado em desenvolvimento de
               software, hardware e sistemas embarcados.\",
               \"hash_arquivo\": \"
               e3b0c44298fc1c149afbf4c8996fb\"}",
        }
    ]
}
```

2. **Banco de Dados:**

   Para armazenar e gerenciar os dados das credenciais de forma eficiente, utilizamos um banco de dados PostgreSQL.É um sistema de gerenciamento de banco de dados relacional (SGBDR) avançado e de código aberto, conhecido por sua robustez, desempenho e conformidade com os padrões SQL. O banco de dados é integrado à API Ruby on Rails, permitindo o armazenamento seguro e a recuperação rápida dos dados necessários para as operações de credenciamento.

   Com base nos requisitos funcionais definidos, foi criado um esquema de banco de dados (Figura 4) para suportar as operações necessárias do sistema. Este diagrama ilustra a estrutura do banco de dados, incluindo tabelas, colunas e relacionamentos que foram projetados para armazenar e gerenciar as credenciais de forma eficiente e segura.

Figura 4 – Ilustração representativa do diagrama de banco de dados



Fonte: Elaborado pelos autores

3. **Blockchain Ethereum e Solana:**

   Inicialmente é feita à criação de contratos inteligentes que serão implantados nas redes Ethereum e Solana. Esses contratos são essenciais para garantir a execução segura e transparente das operações relacionadas à geração, edição e remoção de credenciais. Na rede Ethereum, aproveitamos a flexibilidade e a ampla adoção dessa blockchain, enquanto na rede Solana, priorizamos a escalabilidade e a baixa latência.

   A seguir está exemplificado o pseudo-código dos contratos desenvolvidos:

```
algoritmo "Contrato de Credenciais"

estrutura Credencial
    id, nome, id_instituicao, autor, metadados, id_evento:
        texto
fim-estrutura

variavel credenciais: dicionario<texto, Credencial>

procedimento adicionarCredencial(id, nome, id_instituicao,
    autor, metadados, id_evento: texto)
    credenciais[id] = Credencial{id, nome, id_instituicao,
        autor, metadados, id_evento}
fim-procedimento

procedimento editarCredencial(id, nome, id_instituicao, autor
    , metadados, id_evento: texto)
    credenciais[id] = Credencial{id, nome, id_instituicao,
        autor, metadados, id_evento}
fim-procedimento

procedimento removerCredencial(id: texto)
    apagar credenciais[id]
fim-procedimento

fim-algoritmo
```

   A estrutura é descrita da seguinte forma:

   - **Estrutura Credencial:** Define os campos essenciais (id, nome, id da instituicao, autor, metadados, id do evento) de uma credencial.

- **Variável Credenciais:** Um dicionário que armazena as credenciais utilizando o id como chave.
- **Procedimento adicionarCredencial:** Adiciona uma nova credencial ao dicionário.
- **Procedimento editarCredencial:** Atualiza uma credencial existente no dicionário.
- **Procedimento removerCredencial:** Remove uma credencial do dicionário.

Essa estrutura permite gerenciar de forma eficiente as operações de criação, edição e remoção de credenciais. Este padrão foi seguido para a implementação dos contratos na Ethereum usando Solidity e na Solana usando Rust, sendo ambos adicionados às suas respectivas blockchains.

As figuras apresentadas ilustram as saídas do terminal em duas etapas cruciais do desenvolvimento do sistema de certificação baseado em blockchain. A Figura 5 mostra a saída do terminal no momento em que o contrato inteligente foi implementado na rede Ethereum utilizando a linguagem Solidity. Já a Figura 6 apresenta a saída do terminal durante a execução de uma transação com base no contrato inteligente implementado, demonstrando a interação prática com a blockchain.

Figura 5

```
Deploying 'CredentialsContract'
-------------------------------
> transaction hash:    0xb3fcb2e00c88b05768bdc2c43d9d41610cc2e6dfdd588589f5e0f4682cdbb9bd
> Blocks: 0            Seconds: 0
> contract address:    0x81cc886Be1A38d9D1D6EEfdeCA90dC03C09647C0
> block number:        1
> block timestamp:     1723751905
> account:             0xB7B5D5eb9B8fBC5828FAd8065663dF0E19196467
> balance:             999.998122659625
> gas used:            556249 (0x87cd9)
> gas price:           3.375 gwei
> value sent:          0 ETH
> total cost:          0.001877340375 ETH
```

Log da implantação contrato na rede ethereum. Fonte: Elaborado pelos autores

Figura 6

```
Transaction: 0x4b0c66cd2fdbe50abe7f8e4a1296fb2ea97f0a7a8045547a01ccbe3d75596a71
Gas usage: 37508
Block number: 12
Block time: Thu Aug 15 2024 17:00:10 GMT-0300 (Horário Padrão de Brasília)
```

Log da transação de uma credencial na rede ethereum. Fonte: Elaborado pelos autores

4.4 Fluxo do Evento

Para lidar com o evento, utilizamos o padrão de projeto State, que é um dos padrões comportamentais definidos no livro (GAMMA *et al.*, 1994). Esse padrão permite que um objeto altere seu comportamento quando seu estado interno muda. Isso é alcançado por meio da criação de classes que representam diferentes estados possíveis para esse objeto e permitindo que o objeto mude de uma classe de estado para outra conforme necessário como demonstrado na figura 7.

O funcionamento de cada estado é descrito a seguir:

1. **Em Revisão**

   Nesta fase inicial, os usuários da instituição podem criar, editar e remover eventos com todas as informações necessárias. Há também uma validação preliminar dos metadados antes de salvar os dados.

2. **Aprovado ou Rejeitado**

   O administrador da instituição verifica os metadados do evento. Ele pode aprovar ou rejeitar o evento, fornecendo uma justificativa em caso de rejeição.

   Durante estas estapas é possível conecta-se às blockchains Ethereum ou Solana para calcular uma estimativa do custo das operações para gerar, editar ou remover credenciais.

3. **Em Execução**

   As credenciais do evento são implementadas nas redes Ethereum ou Solana, conforme escolhido pela instituição. O sistema registra todas as transações e interações com a blockchain.

4. **Concluído**

   O estado "Concluído"indica que todas as operações de credenciais foram bem-sucedidas e registradas na blockchain. As credenciais são disponibilizadas publicamente para acesso e verificação.

5. **Parcialmente Concluído**

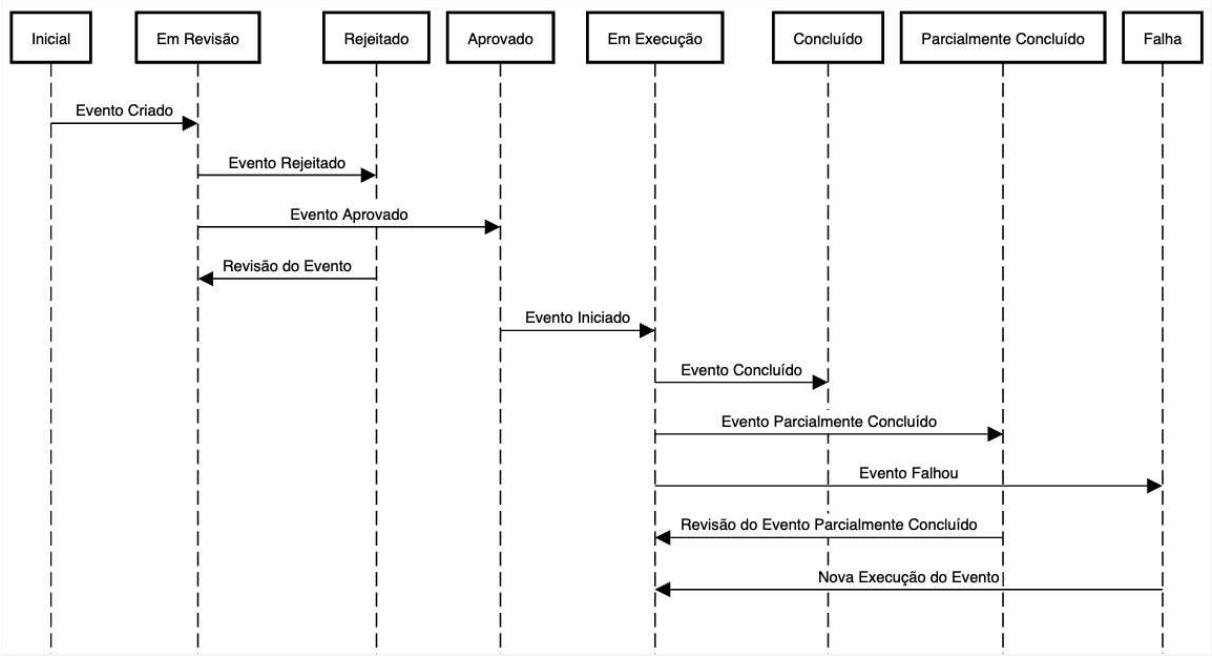
   O estado "Parcialmente Concluído"ocorre quando algumas credenciais não foram atualizadas com sucesso. O usuário é notificado sobre as credenciais que falharam e pode iniciar um novo fluxo para corrigir as pendências.

6. **Falha**

   O estado "Falha"ocorre quando uma operação não pode ser concluída. Isso pode acontecer devido a falhas de conexão, erros nos dados ou restrições de segurança. O sistema registra o

incidente e notifica os usuários para que possam resolver o problema e reiniciar o processo, se necessário.

Figura 7 – Ilustração representativa do fluxo de estados dos eventos

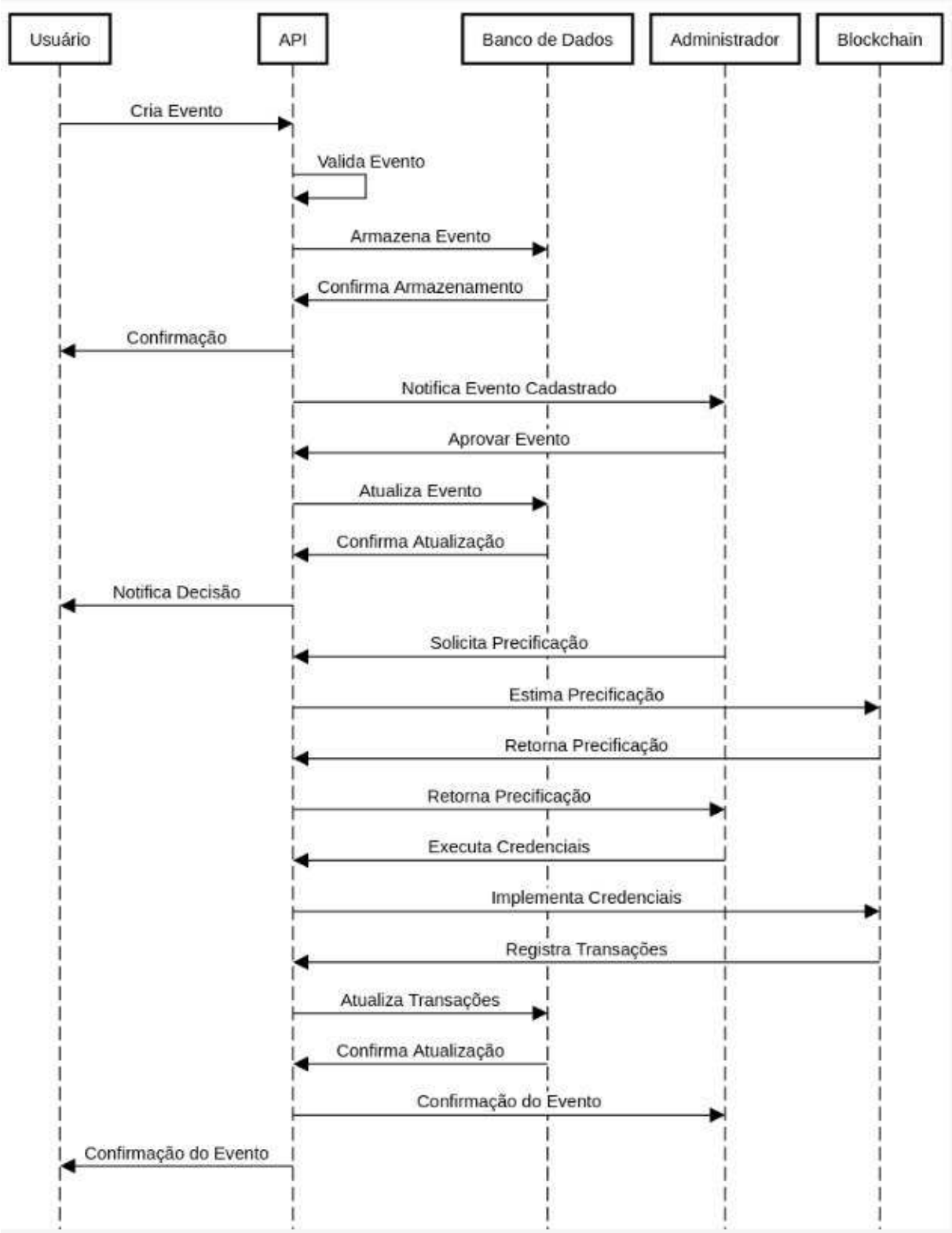


Fonte: Elaborado pelos autores

Fluxo do Completo da Aplicação

No processo de criação e aprovação de um evento, os diferentes componentes interagem conforme ilustrado na Figura 8. Esta figura detalha como o usuário, a API, o banco de dados, o administrador e a blockchain trabalham juntos para garantir que todas as etapas sejam validadas, armazenadas e notificadas adequadamente.

Figura 8 – Ilustração representativa da arquitetura do sistema



Fonte: Elaborado pelos autores

5 EXPERIMENTOS

5.1 Metodologia de experimentação

Neste capítulo, são apresentados os elementos centrais da metodologia empregada para avaliar a ferramenta proposta, com foco na eficiência e nos custos das operações nas redes blockchain Ethereum e Solana para a geração de credenciais digitais. O principal objetivo dos experimentos é investigar e comparar o desempenho dessas duas plataformas em cenários reais de uso, fornecendo respostas claras às questões levantadas pelos objetivos específicos do estudo.

A escolha dos experimentos foi guiada pelos seguintes critérios:

1. **Avaliação de Soluções Blockchain**: Um dos objetivos centrais deste trabalho é analisar diferentes soluções de blockchain para o gerenciamento de certificados digitais. Por isso, foi essencial realizar experimentos que permitissem uma comparação direta entre as redes Ethereum e Solana, considerando a criação, o gerenciamento e a autenticação de credenciais digitais.
2. **Implementação e Integração**: A ferramenta desenvolvida foi integrada com ambas as blockchains, exigindo a criação de cenários de teste que reflitam condições práticas e que possam ser reproduzidos. Estes cenários foram desenhados para medir a eficiência da integração e identificar possíveis desafios e limitações de cada plataforma.
3. **Comparação de Desempenho e Custos**: O experimento busca responder a questões críticas sobre o desempenho e os custos associados às operações em Ethereum e Solana. As métricas coletadas, como logs de transações, tempo de resposta, e custos de transação, são essenciais para uma análise comparativa, proporcionando informações valiosas para desenvolvedores e usuários que desejam escolher a plataforma mais adequada às suas necessidades.

Esses experimentos foram projetados não apenas para cumprir os objetivos específicos do trabalho, mas também para fornecer uma base sólida para a discussão das vantagens e limitações de cada solução blockchain, contribuindo para um entendimento mais profundo das tecnologias envolvidas e do seu potencial no contexto do gerenciamento de certificados digitais.

Ambiente de Teste

Para garantir a precisão e a reprodutibilidade dos resultados, foi configurado um ambiente de teste específico, detalhado na Tabela 2.

Tabela 2 – Características do Equipamento Utilizado

Característica	**Descrição**
Modelo do hardware	82MF
Memória	16 GB de RAM DDR4
Processador	Ryzen 5 5500u
Gráficos	Advanced Micro Devices, Inc. [AMD/ATI] Lucienne (rev c2)
Capacidade de Disco	246G
Nome do SO	Ubuntu 22.04.4 LTS.
Tipo do SO	64 bits
Versão do GNOME	42.9
Sistemas de Janelas	wayland

Fonte: Elaborado pelos autores

Criação de Cenário

Para a realização dos testes, utilizou-se a gem faker no Ruby on Rails para gerar dados simulados de um evento de emissão de diplomas. O cenário envolveu a criação de 100 credenciais de alunos, que foram submetidas a processos de crição nas duas redes distintas: Ethereum e Solana.

As interações com a rede Ethereum foram realizadas utilizando a aplicação Ganache, que é uma ferramenta de desenvolvimento que simula um ambiente local de blockchain, permitindo a execução de contratos inteligentes em um ambiente controlado. Para a rede Solana, os testes foram conduzidos usando os recursos de simulação oferecidos pela própria infraestrutura da rede Solana. Esses ambientes permitiram replicar as condições reais de operação, garantindo que os resultados fossem representativos das operações em produção.

Métricas Coletadas

Estas métricas são cruciais para entender o comportamento da ferramenta e realizar uma análise das operações nas redes blockchain.

1. **Logs de Transações:** Registro detalhado de todas as transações realizadas nas redes blockchain.
2. **Métricas de Performance:** Monitoramento do tempo de resposta durante a execução

das operações.

3. **Custos de Transação:** Coleta dos custos associados a cada operação nas redes Ethereum e Solana.

Período da Coleta de Dados

Tabela 3 – Credenciais Geradas por Dia e Turno nas Redes Ethereum e Solana

Data	**Turno**	**Ethereum**	**Solana**
20/05/2024	Manhã (8-12h)	100	100
20/05/2024	Tarde (12-17h)	100	100
20/05/2024	Noite (17-23h)	100	100
21/05/2024	Manhã (8-12h)	100	100
21/05/2024	Tarde (12-17h)	100	100
21/05/2024	Noite (17-23h)	100	100
22/05/2024	Manhã (8-12h)	100	100
22/05/2024	Tarde (12-17h)	100	100
22/05/2024	Noite (17-23h)	100	100
23/05/2024	Manhã (8-12h)	100	100
23/05/2024	Tarde (12-17h)	100	100
23/05/2024	Noite (17-23h)	100	100
24/05/2024	Manhã (8-12h)	100	100
24/05/2024	Tarde (12-17h)	100	100
24/05/2024	Noite (17-23h)	100	100

Dados fornecidos pelo autor.

Durante um período de uma semana, os testes no cenário definido foram realizados em três turnos diários: manhã (8-12h), tarde (12-17h) e noite (17-23h). A Tabela 3 apresenta uma visão detalhada das credenciais geradas em cada turno para ambos os blockchains.

Observações

- **Consistência dos Testes**: Em cada dia, o número de credenciais geradas foi exatamente igual para ambos os blockchains e permaneceu constante ao longo dos turnos.
- **Turnos de Coleta**: A divisão dos turnos em manhã, tarde e noite permite observar possíveis variações no desempenho e nos custos das transações de acordo com diferentes horários, o que pode ser influenciado pela carga da rede e outros fatores temporais.
- **Período de Coleta**: A coleta de dados foi realizada de 20/05/2024 a 24/05/2024. Essa janela temporal permite capturar variações diárias e padrões repetitivos.

Implicações

- **Análise de Desempenho e Custos**: Com os dados coletados, é possível analisar o desempenho e os custos das transações em Ethereum e Solana, considerando a influência dos diferentes turnos.
- **Planejamento de Uso**: Para desenvolvedores e usuários dessas redes, entender as variações de desempenho e custos ao longo do dia pode ajudar no planejamento de atividades e na otimização de recursos, escolhendo os horários mais eficientes para realizar transações.

5.2 Resultados

Esta seção, mostra os resultados dos estudos de caso elaborados na seção de metodologia de experimentação.

Análise do Tempo de Execução de Ethereum e Solana

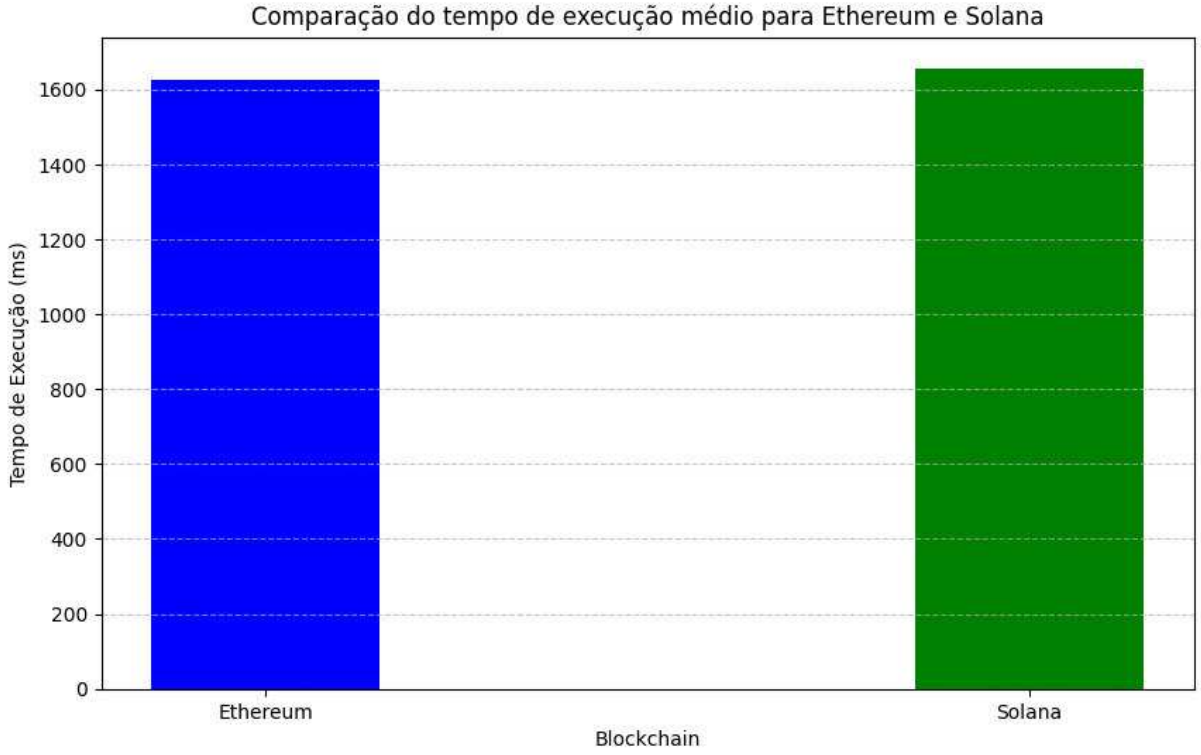
Blockchain	Tempo de Execução Médio (ms)	Desvio Padrão (ms)	Intervalo de Confiança 95% (ms)
Ethereum	1625,44	94,44	(360,96, 398,62)
Solana	1656,89	101,22	(670,78, 746,26)

Tabela 4 – Comparação do tempo de execução médio, desvio padrão e intervalo de confiança para Ethereum e Solana.

A Tabela 4 apresenta a comparação do tempo de execução médio de transações entre as blockchains Ethereum e Solana. Temos que a Solana apresenta um tempo de execução médio aproximadamente 1,94% maior do que Ethereum, sugerindo que, em termos de latência, elas oferecem desempenhos similares.

Além disso, ao observar o desvio padrão, é possível notar que a variação no tempo de execução para ambas as blockchains é relativamente baixa, com Solana apresentando uma variação ligeiramente maior do que Ethereum. Isso indica que, embora Solana tenha um tempo de execução médio um pouco maior, ela também apresenta uma maior dispersão dos tempos de execução em relação à média. Quanto ao intervalo de confiança de 95%, apesar das médias próximas, Solana tem uma maior incerteza associada ao seu tempo de execução médio, o que pode ser relevante ao considerar a consistência da performance das duas blockchains.

Figura 9 – Comparação do tempo de execução médio para Ethereum e Solana.



Fonte: Elaborado pelos autores

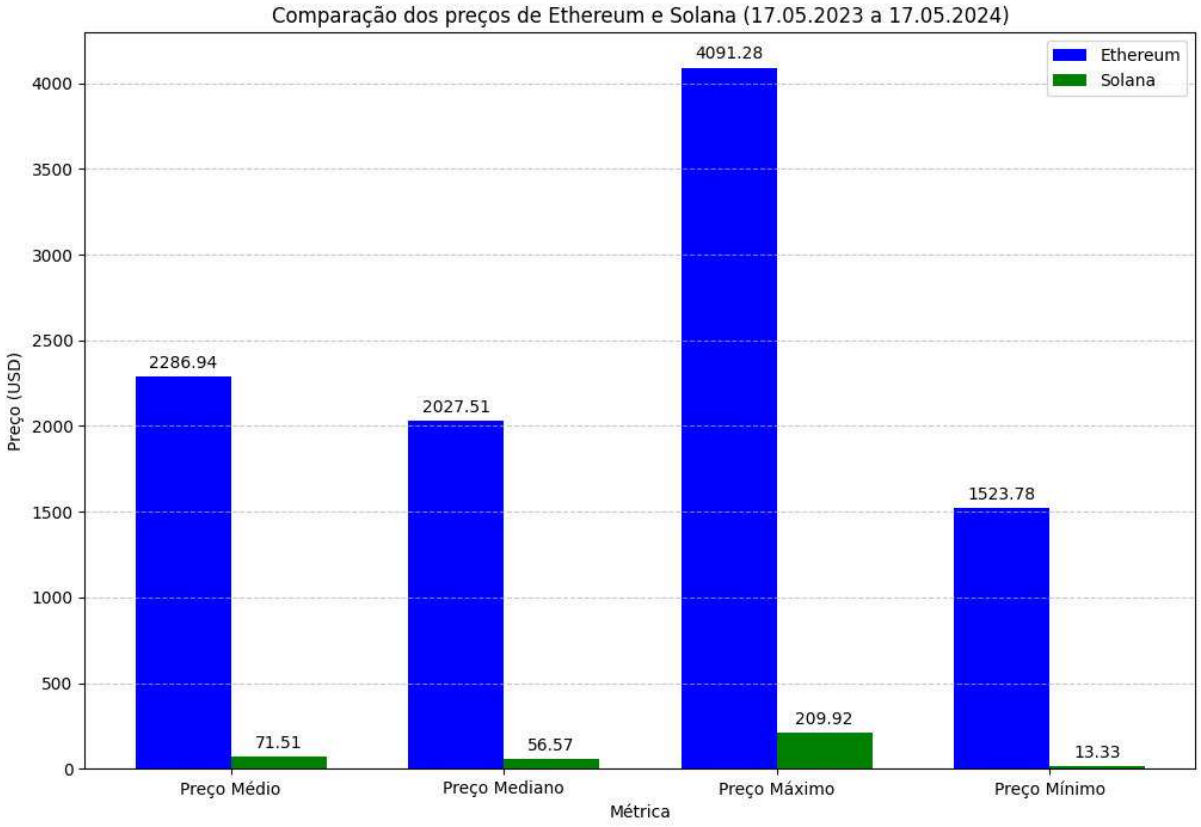
Análise de Preços de Ethereum e Solana

Métrica	Ethereum (USD)	Solana (USD)
Preço Médio	2.286,94	71,51
Preço Mediano	2.027,51	56,57
Preço Máximo	4.091,28	209,92
Preço Mínimo	1.523,78	13,33

Tabela 5 – Comparação dos preços de Ethereum e Solana no período de 17.05.2023 a 17.05.2024.

A Tabela 5 e a Figura 10 mostram que o preço médio do Ethereum é significativamente mais alto que o do Solana. O preço médio do Ethereum é aproximadamente 3100% maior que o do Solana, e essa disparidade se reflete também nos preços máximo e mínimo. Isso sugere que o Ethereum possui uma volatilidade de preço mais elevada, o que pode influenciar na percepção de risco e na decisão de investimento.

Figura 10 – Comparação dos preços de Ethereum e Solana no período de 17.05.2023 a 17.05.2024.



Fonte: Elaborado pelos autores

Análise do Custo de Transações Ethereum e Solana

Métrica	Valor Médio	Desvio Padrão	Intervalo de Confiança 95%
Gás (Ethereum)	45.057,84	4.025,19	(44.255,13; 45.860,55)
Lamports (Solana)	5.000,00	0,00	(5.000,00; 5.000,00)

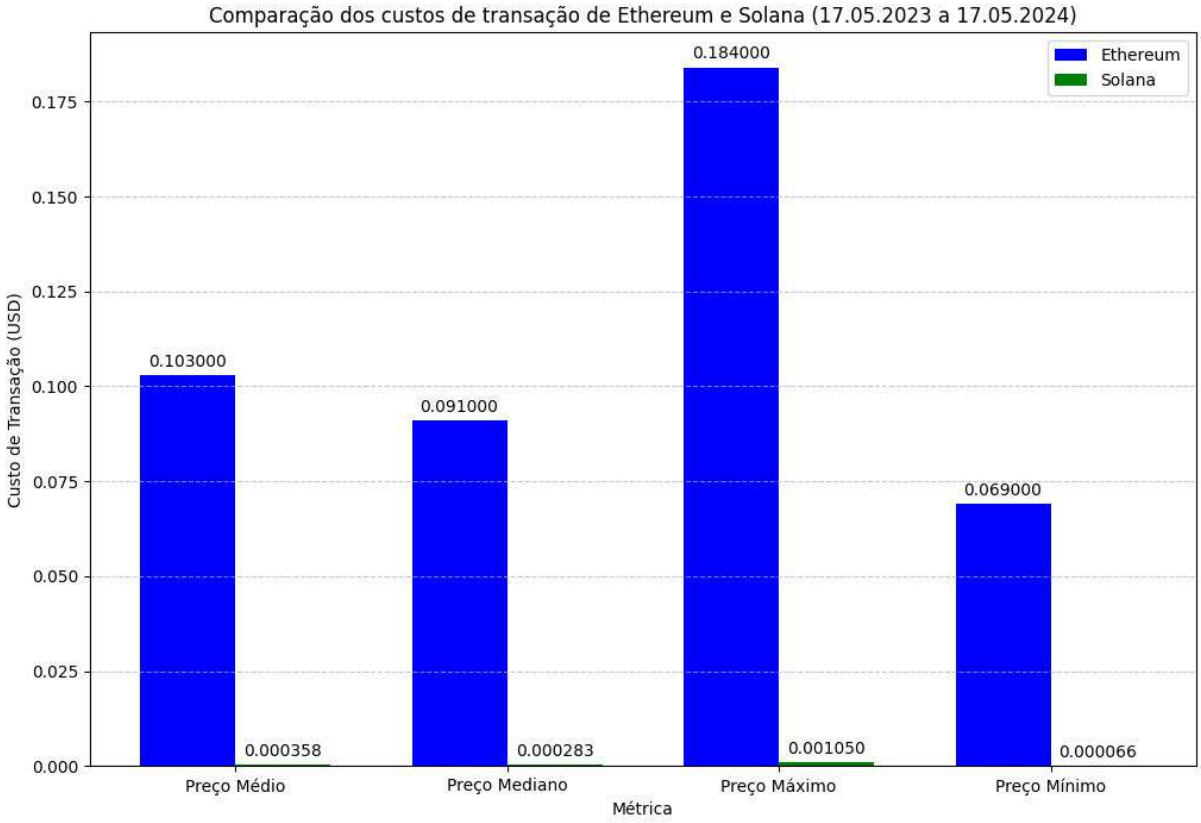
Tabela 6 – Média, desvio padrão e intervalo de confiança de 95% para o gás do Ethereum e Lamports do Solana.

Métrica	Custo Transação Ethereum (USD)	Custo Transação Solana (USD)
Preço Médio	$0,103	$0,000358
Preço Mediano	$0,091	$0,000283
Preço Máximo	$0,184	$0,00105
Preço Mínimo	$0,069	$0,000066

Tabela 7 – Comparação dos custos de transação de Ethereum e Solana no período de 17.05.2023 a 17.05.2024 em dólares.

A Tabela 7 compara os custos das transações em termos de dólares americanos, revelando que o custo médio de transação no Ethereum ($0,103) é consideravelmente mais alto que no Solana ($0,000358), representando uma diferença de aproximadamente 28700%. Essa

Figura 11 – Comparação dos custos de transação de Ethereum e Solana no período de 17.05.2023 a 17.05.2024 em dólares.



Fonte: Elaborado pelos autores

diferença é consistente nas métricas de custo máximo e mínimo, reforçando a conclusão de que Solana oferece uma solução mais econômica para a realização de transações.

Ao analisar a Tabela 6, observamos que o desvio padrão do custo de gás no Ethereum é relativamente alto (4.025,19 Gwei), indicando uma variação considerável nos custos das transações ao longo do tempo. Isso reflete a natureza volátil das taxas de gás no Ethereum, que podem flutuar significativamente em resposta à demanda na rede. Em contraste, o valor de Lamports no Solana permanece constante, com um desvio padrão de 0,00, indicando uma estabilidade total nos custos de transação. O intervalo de confiança de 95% para o custo de gás no Ethereum, que varia entre 44.255,13 e 45.860,55 Gwei, sugere que, embora exista variação, o custo tende a se manter dentro de um intervalo relativamente estreito. Esses resultados demonstram a diferença fundamental entre as duas blockchains, onde Ethereum apresenta custos de transação mais voláteis, enquanto Solana oferece uma previsibilidade e estabilidade muito maiores.

Custo no Cenário de Emissão de Diplomas

Métrica	Valor
Universidade	UFC
Período	2023.1
Cursos	123
Concluintes	1380

Tabela 8 – Dados obtidos no painel da Universidade Federal do Ceará (UFC) sobre graduações no período 2023.1. Fonte: paineis.ufc.br.

Métrica	Custo Total Transações Ethereum (BRL)	Custo Total Transações Solana (BRL)
Custo Total	R$739,97	R$2,57

Tabela 9 – Custo no Cenário de Emissão de Diplomas para Ethereum e Solana. A data de colação de grau foi 06 de outubro de 2023, conforme o calendário universitário da UFC, e o valor da conversão foi obtido do site idealsoftwares.com.br.

A Tabela 8 apresenta os dados de graduação da Universidade Federal do Ceará (UFC) para o período 2023.1, com 123 cursos e 1380 concluintes. Ao analisar o custo total das transações no cenário de emissão de diplomas, conforme mostrado na Tabela 9, observa-se uma diferença significativa. O custo total das transações em Ethereum O custo por transação em Ethereum é de R$ 739,97, enquanto em Solana é de apenas R$ 2,57. A diferença percentual entre os custos demonstra que o Ethereum é aproximadamente 28.678% mais caro do que o Solana.

Limitações da Estratégia de Agrupamentos

Durante a implementação do sistema, discutimos outra abordagem visando agrupar credenciais como uma estratégia para minimizar os custos de uma operação. Entretanto, identificamos limitações significativas nessa estratégia.

Blockchain	Máxima Quantidade de Credenciais Agrupadas	Custo
Ethereum	20	11.963.128 (Gwei)
Solana	4	5.000 (Lamports)

Tabela 10 – Comparação de custo para agrupamento de credenciais entre Ethereum e Solana.

No teste realizado na tabela 10, limitamos a passar o hash do arquivo que representa a credencial física, além do nome do aluno, matrícula, nome da instituição e nome da credencial.

Entretanto, é importante observar que esses resultados podem variar dependendo da quantidade de dados envolvidos em cada credencial. O teste realizado limitou os da-

dos a informações essenciais, mas em aplicações reais, a quantidade de dados pode ser significativamente maior, exacerbando as limitações de custo e tamanho mencionadas.

1. **Custo Alto ou Limitado**

   Observamos que o custo total da operação frequentemente se tornava muito mais alto do que as transações individuais. Além disso, em muitos casos, o agrupamento atingia o limite máximo de custo de uma operação em blockchain, impedindo o agrupamento de um volume maior de credenciais.

2. **Restrição de Tamanho**

   A quantidade de informação que pode ser alocada em uma única transação é outra limitação significativa. Essa restrição impacta diretamente a capacidade de agrupar credenciais, especialmente quando essas credenciais contêm uma quantidade considerável de dados.

5.3 Ameaças à Validade

Apesar dos esforços para garantir a precisão e a reprodutibilidade dos resultados, existem algumas ameaças à validade que devem ser observadas:

1. **Ambiente de Teste Limitado:** Os testes foram realizados em um ambiente de teste local específico, que pode divergir de um ambiente de produção. Fatores como conectividade de rede, carga de trabalho e configurações de segurança podem impactar os resultados em um ambiente real.
2. **Falta de Testes de Estresse:** Não foram conduzidos testes de estresse que simulassem cargas extremas de transações ou condições adversas.
3. **Ausência de Arquiteturas de Contêineres e Nuvem:** A infraestrutura utilizada para os testes não incluiu arquiteturas de contêineres (como Kubernetes) ou plataformas de nuvem (AWS, Google Cloud, Azure). A execução em ambientes de contêineres ou em diferentes provedores de nuvem poderia fornecer informações sobre escalabilidade e desempenho.
4. **Limitações na Quantidade de Dados e Operações:** Os testes foram limitados a um conjunto específico de operações e volumes de dados. Em aplicações reais, volumes maiores de dados e uma variedade mais ampla de operações podem impactar os resultados de desempenho e custo.

6 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho teve como objetivo desenvolver uma aplicação para gerenciar e autenticar certificados utilizando a tecnologia blockchain. A motivação surgiu da necessidade de solucionar problemas nos métodos tradicionais de emissão e verificação de certificados acadêmicos, como a dependência de terceiros e vulnerabilidades de armazenamento.

Os objetivos específicos incluíram a criação de um sistema robusto contra falsificações, a facilitação de um processo de validação ágil e confiável, e a avaliação das blockchains Ethereum e Solana para implementação de contratos inteligentes. Desenvolvemos uma aplicação utilizando a infraestrutura das blockchains Ethereum e Solana para garantir a integridade dos certificados, implementando funcionalidades para a emissão e verificação digitais. Além disso, realizamos testes comparativos entre as redes para analisar seu desempenho e viabilidade.

Os resultados demonstraram que tanto Ethereum quanto Solana possuem tempos de execução similares, com uma diferença pequena e pouco significativa na prática. No entanto, a análise dos custos de transação revelou que Solana é significativamente mais econômica que Ethereum, apresentando uma diferença de custo médio de aproximadamente 28.700% durante o período analisado. Essas descobertas são cruciais para orientar futuras implementações e decisões de uso, destacando a viabilidade econômica de Solana para transações em blockchain e seu uso na geração de credenciais estudantis.

Os resultados deste estudo têm um impacto significativo para instituições acadêmicas e organizações envolvidas na emissão e verificação de certificados. Ao utilizar tecnologias como Ethereum e Solana, espera-se que indivíduos e organizações possam verificar as credenciais de alunos atuais e ex-alunos de maneira rápida e segura. A segurança se deve à adoção da tecnologia blockchain, que garante a integridade e a autenticidade das credenciais emitidas. Professores e instrutores poderão solicitar e emitir certificados digitais de cursos ministrados de forma eficiente, destacando-se como alguns dos benefícios concretos da implementação desta ferramenta.

6.1 Trabalhos Futuros

Para futuros desenvolvimentos, é necessário focar na escalabilidade da aplicação, propondo infraestrutura e arquitetura que suportem um crescimento eficiente. Recomenda-se explorar plataformas líderes como Amazon Web Services (AWS), Microsoft Azure e Google Cloud, junto com soluções de código aberto como Kubernetes, para oferecer escalabilidade

horizontal e vertical conforme necessário. Além disso, é importante considerar a integração com novas blockchains emergentes, como Polkadot e Cardano, para diversificar as opções e potencialmente reduzir custos operacionais e de transação.

REFERÊNCIAS

CHENG, D.; CHUANG, C.; HUNG, Y. Application of ethereum smart contract: An extensive survey. **Symmetry**, v. 10, n. 10, p. 470, 2018. Disponível em: <https://www.mdpi.com/2073-8994/10/10/470>.

EZELL, A.; BEAR, J. **Degree mills: The billion-dollar industry that has sold over a million fake diplomas**. [S.l.: s.n.], 2005.

FREEMAN, E. Head first design patterns. **Design Patterns Journal**, v. 4, n. 3, p. 34–56, 2013.

GAMMA, E.; HELM, R.; JOHNSON, R.; VLISSIDES, J. **Design Patterns: Elements of Reusable Object-Oriented Software**. [S.l.: s.n.], 1994.

GRECH, A.; CAMILLERI, A. F. **Blockchain in Education**. [S.l.: s.n.], 2017.

GRESCH, J.; RODRIGUES, B.; SCHEID, E. J.; KANHERE, S. S. The proposal of a blockchain-based architecture for transparent certificate handling. In: **1st Workshop on Blockchain and Smart Contract Technologies (BSCT 2018)**. [S.l.: s.n.], 2018.

HANSSON, D. H. Ruby on rails. **Ruby on Rails Journal**, v. 1, n. 1, p. 1–10, 2008.

HOLOTESCU, C. Understanding blockchain opportunities and challenges. In: **Proc of. International Scientific Conference on eLearning and Software**. Bucharest, Romania: [s.n.], 2018. v. 4, p. 275–283.

JIRGENSONS; KAPENIEKS. Journal of teacher education for sustainability. **Journal of Teacher Education for Sustainability**, v. 20, n. 1, p. 146, 2018.

JIRGENSONS; KAPENIEKS. Journal of teacher education for sustainability. **Journal of Teacher Education for Sustainability**, v. 20, n. 1, p. 147, 2018.

LIN, I. C.; LIAO, Y. C. A survey of blockchain security issues and solutions. **IET Cyber-Physical Systems: Theory & Applications**, v. 1, n. 1, p. 13–27, 2017.

NOFER, M.; GOMBER, P.; HINZ, O.; SCHIERECK, D. Blockchain. **Business & Information Systems Engineering**, v. 59, n. 3, p. 183–187, 2017.

OLIVER, M.; MOREN, J.; PRIETO, G.; BENITEZ, D. Using blockchain as a tool for tracking and verification of official degrees: business model. In: **29th European Regional Conference of the International Telecommunications Society (ITS). Towards a Digital Future: Turning Technology into markets**. [S.l.: s.n.], 2018.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World**. [S.l.]: Penguin Random House, 2016.

TARIQ, A.; HAQ, H. B.; ALI, S. T. Cerberus: A blockchain-based accreditation degree verification system. dez. 2019.

TRUKANOVIC, M.; HOLBL, M.; KOSIC, K.; HERICKO, M.; KAMISALIC, A. Eductx: A blockchain-based higher education credit platform. **IEEE Access**, v. 6, p. 5112–5127, jan. 2018.

University of Nicosia. **Academic Certificates on the Blockchain**. <http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/>. Accessed: 17 de junho de 2024.

ZHENG, Z.; XIE, S.; DAI, H.; CHEN, X.; WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE. **2017 IEEE International Congress on Big Data**. [S.l.], 2017. p. 557–564.