

**CENTRO FEDERAL DE EDUCACÃO TECNOLÓGICA
CELSO SUCKOW DA FONSECA**

**Aplicação de Tecnologias Descentralizadas para
Gestão de Registros Acadêmicos e Transferência de
Créditos**

Gabriel Franco Barreto Cavalcanti

Gilmar Santos Neto

Juan Carvalho Silva de Lima

Prof. Orientador:

Diogo Silveira Mendonça

**Rio de Janeiro,
Janeiro de 2026**

**CENTRO FEDERAL DE EDUCACÃO TECNOLÓGICA
CELSO SUCKOW DA FONSECA**

Aplicação de Tecnologias Descentralizadas para Gestão de Registros Acadêmicos e Transferência de Créditos

Gabriel Franco Barreto Cavalcanti

Gilmar Santos Neto

Juan Carvalho Silva de Lima

Projeto final apresentado em cumprimento às
normas do Departamento de Educação
Superior do Centro Federal de Educação
Tecnológica Celso Suckow da Fonseca,
CEFET/RJ, como parte dos requisitos para
obtenção do título de Bacharel em Ciência da
Computação.

Prof. Orientador:

Diogo Silveira Mendonça

**Rio de Janeiro,
Janeiro de 2026**

DEDICATÓRIA

Dedicamos este trabalho às nossas famílias,
cuja presença, amor e inspiração nos
acompanham diariamente. Esta conquista é
também de vocês.

AGRADECIMENTOS

Gostaríamos de manifestar nosso profundo agradecimento a todos que, de alguma forma, contribuíram para a concretização deste trabalho. Agradecemos, em especial, à nossa família, pelo apoio constante e incentivo em cada etapa da jornada. Estendemos nossa gratidão ao orientador, Diogo Mendonça, por sua dedicação, orientação e contribuições valiosas, bem como aos professores que compartilharam conhecimento ao longo do percurso. A todos que, direta ou indiretamente, fizeram parte dessa caminhada, deixamos aqui nosso sincero muito obrigado.

RESUMO

Os registros acadêmicos, tradicionalmente centralizados pelas instituições de ensino, enfrentam diversos problemas estruturais, como risco de perda de dados, lentidão no acesso, burocracia excessiva, falta de interoperabilidade entre sistemas, baixa transparência, e limitação no controle do aluno sobre suas informações. Diante disso, este trabalho propõe o aprimoramento da prova de conceito de um sistema descentralizado de gestão de registros acadêmicos com o objetivo de fornecer maior viabilidade técnica e funcional da solução proposta por meio da superação das limitações identificadas no trabalho-base. Portanto, espera-se, assim, que a adoção desse modelo reduza a dependência de intermédios institucionais, agilize processos de transferência de créditos e consulta de históricos, e proporcione ao aluno controle permanente sobre seus dados. Dessa forma, este trabalho busca não apenas apresentar o aperfeiçoamento de um aditivo tecnológico inovador para a gestão acadêmica, mas também a abertura de caminhos para futuras implementações e considerações que promovam maior transparência, segurança e autonomia no setor educacional.

Palavras-chave: blockchain; smart contracts; gestão de registros acadêmicos; ensino superior; aproveitamento de créditos

ABSTRACT

Academic records, traditionally centralized by educational institutions, face several structural problems, such as risk of data loss, slow access, excessive bureaucracy, lack of interoperability between systems, low transparency, and limited student control over their information. In view of this, this work proposes the improvement of the proof of concept of a decentralized academic records management system with the aim of providing greater technical and functional viability of the proposed solution, overcoming the limitations identified in the baseline work. Therefore, it is expected that the adoption of this model will reduce dependence on institutional intermediaries, streamline the processes of credit transfer and consultation of academic records, and provide students with permanent control over their data. Thus, this work seeks not only to present the improvement of an innovative technological additive for academic management, but also to pave the way for future implementations and considerations that promote greater transparency, security, and autonomy in the educational sector.

Keywords: blockchain; smart contracts; academic records management; higher education; credit transfer

SUMÁRIO

1	Introdução	1
2	Fundamentação teórica	3
2.1	Blockchain	3
2.2	Rede Ethereum	4
2.3	Redes EVM-Compatible	6
2.4	Carteiras de usuário e padrões de conectividade em aplicações descentralizadas	6
2.5	Processamento em lote	7
2.6	Criptografia aplicada à proteção de dados	8
2.7	Gestão de identidade e controle de acesso em ambientes distribuídos	9
3	Trabalhos relacionados	11
4	Desenvolvimento	16
4.1	Cenário de negócio e processos acadêmicos	16
4.2	O sistema-base da prova de conceito	17
4.3	Limitações do sistema-base	20
4.4	Concepção da solução	21
4.5	Modelagem do sistema	23
4.5.1	Aplicação de escalabilidade ao contrato inteligente	23
4.5.2	Serviço de processamento em lote para ingestão de registros	26
4.5.3	Solução criptográfica e modelo de controle condicional de registros	27
4.5.4	Abstração de complexidade via carteiras embarcadas e protocolos de autenticação social	31
4.5.5	Infraestrutura em rede EVM-Compatible para viabilidade econômica	34
5	Avaliação experimental e resultados	35
5.1	Metodologia e ambiente de testes	35
5.2	Demonstração do funcionamento e fluxo operacional do DApp	36
5.3	Desempenho do serviço de orquestração em lote	39
5.4	Análise de segurança e qualidade do contrato inteligente	41
5.5	Análise comparativa de custos e escalabilidade	43

5.6	Discussão dos resultados	44
6	Conclusão	46
	Referências Bibliográficas	47

LISTA DE FIGURAS

FIGURA 1:	Cadeia de blocos em uma rede blockchain [Nakamoto, 2008]	3
FIGURA 2:	Arquitetura do UniverCert [Kistabayev et al., 2023]	14
FIGURA 3:	Diagrama de classes de Pedrosa et al. [2025]	18
FIGURA 4:	Arquitetura geral do sistema descentralizado de registro acadêmico	22
FIGURA 5:	Fluxo criptográfico da instituição e geração de chave pública	28
FIGURA 6:	Fluxo criptográfico de registro do estudante	29
FIGURA 7:	Fluxo de solicitação de acesso pelo visitante	30
FIGURA 8:	Fluxo de recifragem e concessão de acesso	31
FIGURA 9:	Fluxo universal de decifragem de dados	32
FIGURA 10:	Interface de autenticação com suporte a login social e geração de carteira embarcada.	36
FIGURA 11:	Processo de autorização institucional realizado pelo administrador do contrato.	37
FIGURA 12:	Processo de cadastro das informações da instituição de ensino.	37
FIGURA 13:	Tela da instituição com botões para ingestão em lote	38
FIGURA 14:	Interface de preenchimento e cifragem de dados pessoais pelo estudante.	38
FIGURA 15:	Confirmação de execução das operações de batching na blockchain.	38
FIGURA 16:	Painel de visualização do histórico acadêmico decifrado localmente pelo aluno.	39
FIGURA 17:	Interface do visitante para requisição de acesso a registros de terceiros.	39
FIGURA 18:	Processo do aluno conceder acesso aos registros acadêmicos para o visitante.	40

LISTA DE TABELAS

TABELA 1:	Síntese crítica dos trabalhos relacionados	15
TABELA 2:	Tabela dos requisitos funcionais	18
TABELA 3:	Resultados consolidados dos testes de desempenho (em segundos)	41
TABELA 4:	Comparativo de custos transacionais detalhado: <i>Ethereum</i> vs. <i>Polygon</i> (cenário 1)	43
TABELA 5:	Estimativa de custos totais na rede <i>Polygon</i> considerando a fragmentação por <i>chunks</i>	44

LISTA DE ABREVIACÕES

DAGS	Directed Acyclic Graphs	26
ECDSA	Elliptic Curve Digital Signature Algorithm	9
ECIES	Elliptic Curve Integrated Encryption Scheme	8, 28
IOT	Internet Das Coisas	3
IPFS	InterPlanetary File System	12
LGPD	Lei Geral De Proteção De Dados	12
PBKDF2	Password-Based Key Derivation Function 2	9

Capítulo 1

Introdução

Os registros acadêmicos desempenham um papel fundamental na trajetória educacional dos alunos, pois documentam notas, créditos, matrículas e vínculos institucionais que validam juridicamente seu progresso acadêmico. Atualmente, a gestão desses dados permanece em grande parte centralizada nas próprias instituições de ensino, o que gera desafios operacionais e estruturais: riscos de perda ou inconsistência de informações, burocracia em processos de transferência de créditos e emissão de diplomas, falta de interoperabilidade entre diferentes sistemas institucionais e, sobretudo, a limitação do controle dos próprios alunos sobre seus dados educacionais.

O impacto dessas fragilidades já se mostrou crítico em casos reais. Em 2014, o descenciamento do Centro Universitário da Cidade (UniverCidade) e da Universidade Gama Filho (UGF) pelo Ministério da Educação expôs milhares de estudantes à impossibilidade de acessar diplomas e históricos acadêmicos. A dependência exclusiva de arquivos físicos e da mediação institucional comprometeu a continuidade de suas trajetórias educacionais e profissionais, evidenciando a vulnerabilidade do modelo centralizado de registros acadêmicos [[Ministério da Educação, 2014](#); [Bom Dia Rio, 2019](#)].

Nesse contexto, a tecnologia blockchain surge como uma alternativa promissora. Suas propriedades de descentralização, imutabilidade e segurança criptográfica possibilitam o armazenamento e compartilhamento confiável de registros acadêmicos, reduzindo a dependência de intermediários e assegurando maior resiliência contra perdas ou manipulações indevidas. Para as instituições, os benefícios incluem maior eficiência nos processos administrativos, transparência na gestão das informações, interoperabilidade entre diferentes universidades e a possibilidade de criar ecossistemas acadêmicos mais abertos e colaborativos. Para os estudantes, a tecnologia devolve autonomia e controle sobre seus históricos, além de simplificar a mobilidade acadêmica nacional e internacional.

Com base nessa perspectiva, [Pedrosa et al. \[2025\]](#) desenvolveram uma prova de conceito de um sistema de gestão acadêmica baseado em blockchain. Esse protótipo, implementado em *Solidity* e executado na rede *Ethereum*, permitia o armazenamento de instituições, alunos, cursos, disciplinas e notas diretamente na blockchain. O sistema demonstrou a viabilidade

técnica da proposta e trouxe ganhos de transparência e rastreabilidade. Entretanto, também revelou limitações importantes: a necessidade de interações manuais em cada transação, o uso de bibliotecas criptográficas hoje depreciadas e os custos elevados de operação devido às taxas de operação (*gas*).

Diante dessas limitações, este trabalho propõe uma evolução dessa prova de conceito, com o objetivo de tornar a solução mais escalável, segura e adequada ao uso em ambientes acadêmicos reais. Para isso, apresenta-se um modelo de ingestão de dados em lote, capaz de reduzir a necessidade de interações manuais; a adoção de uma arquitetura criptográfica híbrida, mais segura e independente de serviços obsoletos; a utilização de redes *EVM-Compatible* de baixo custo, que asseguram maior sustentabilidade econômica; e a introdução de carteiras embarcadas, mecanismo de acessibilidade e usabilidade que simplifica o acesso ao sistema para estudantes e instituições. Assim, este trabalho busca não apenas superar as limitações do protótipo original, mas também avançar em direção a uma solução prática e aplicável, capaz de transformar a forma como registros acadêmicos são geridos, compartilhados e preservados.

Além desta introdução, o trabalho está estruturado em quatro seções principais. A seção 2 aborda os fundamentos teóricos necessários para a compreensão do tema. A seção 3 apresenta e analisa os principais estudos existentes na literatura que abordam a descentralização de registros acadêmicos com blockchain, buscando identificar contribuições relevantes e lacunas presentes. A seção 4 descreve detalhadamente o sistema-base da prova de conceito, suas limitações, a solução, e a modelagem e implementação dessa solução proposta. A seção 5 aborda a análise dos experimentos realizados, comparação de custos, desempenho e segurança. E, por fim, a seção 6 que sintetiza o projeto final e seus resultados, além de apontar perspectivas futuras.

Capítulo 2

Fundamentação teórica

2.1 Blockchain

A Blockchain é uma tecnologia que permite que duas ou mais partes realizem transações digitais de forma segura e transparente, sem a necessidade de um regulador central. Essa característica elimina a dependência de intermediários tradicionais e garante a integridade das informações por meio de mecanismos criptográficos robustos [Nakamoto, 2008]. Além de seu uso inicial no setor financeiro, suas aplicações têm se expandido para áreas como cadeias de suprimentos, saúde, Internet das Coisas (IoT), governança pública, educação e segurança de dados, evidenciando sua versatilidade e potencial de transformação [Fran Casino, 2018]. Ela funciona como um livro-razão digital, distribuído e imutável, no qual todas as transações são registradas em blocos encadeados criptograficamente, garantindo transparência, rastreabilidade e resistência a fraudes na rede. Nakamoto [2008] descreve que os principais mecanismos para fornecer essas garantias são: as transações públicas, a prova de trabalho e o incentivo financeiro.

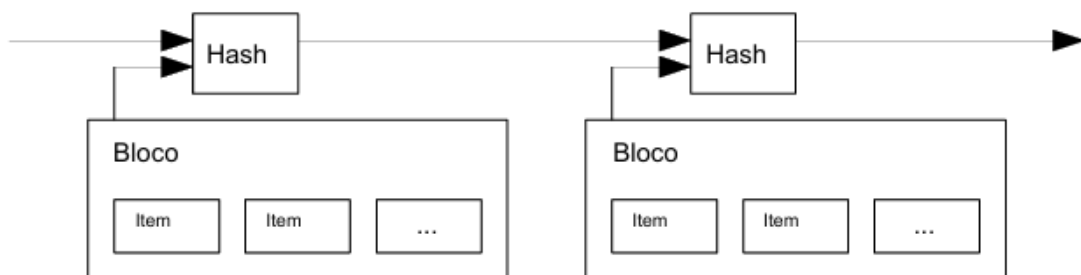


Figura 1: Cadeia de blocos em uma rede blockchain [Nakamoto, 2008]

As transações em redes blockchain públicas garantem a segurança por meio da transparência, permitindo que qualquer participante visualize o histórico completo das operações realizadas. Essa característica dificulta fraudes, como o gasto duplo, uma vez que tentativas de reutilização de valores já consumidos podem ser detectadas e invalidadas pelo mecanismo de consenso, como a Prova de Trabalho (*Proof of Work*). Apesar da transparência, as blockchains

públicas não oferecem anonimato pleno, mas sim pseudonimato, pois os usuários são identificados por endereços criptográficos, e não diretamente por suas identidades reais. Embora não haja uma associação explícita entre endereços e indivíduos, técnicas de análise de transações, correlação de dados externos e metadados podem permitir a reidentificação dos participantes. Dessa forma, observa-se um equilíbrio entre segurança e rastreabilidade, ao custo de limitações inerentes à privacidade em blockchains públicas.

A prova de trabalho (*Proof of Work*) é um mecanismo fundamental para validar e garantir a inclusão segura de blocos na rede blockchain. Seu princípio baseia-se na realização de um intenso esforço computacional para encontrar um valor chamado *nonce*, cujo *hash* resultante deve atender a um critério específico, geralmente iniciando com um determinado número de bits zero. Esse processo assegura que, uma vez validado, o bloco não possa ser alterado sem que todo o trabalho de validação seja refeito, incluindo os blocos subsequentes, o que reforça a imutabilidade da cadeia. Além disso, a prova de trabalho também resolve o problema de consenso de forma robusta, substituindo o modelo "um-IP-um-voto" por uma abordagem baseada em poder computacional, na qual a decisão da maioria é representada pela cadeia mais longa, resultado da maior quantidade de trabalho acumulado, garantindo assim maior segurança e resistência a ataques.

A blockchain também oferece incentivos financeiros aos nós participantes da rede como forma de estimular a validação contínua e segura das transações. Um dos principais incentivos ocorre por meio da primeira transação de cada bloco, conhecida como *coinbase transaction*, que cria uma nova unidade monetária e a destina ao minerador responsável pela criação e validação daquele bloco. Essa recompensa tem como objetivo compensar o esforço computacional e o consumo energético envolvidos no processo de mineração. Outro tipo de incentivo é obtido por meio das taxas de transação (*gas*): sempre que o valor total das saídas de uma transação for inferior ao valor das entradas, a diferença é automaticamente revertida como taxa de transação para o minerador. Dessa forma, o sistema cria um modelo sustentável que combina a emissão controlada de novas moedas com a coleta de taxas, garantindo a manutenção da rede e incentivando a participação ativa dos validadores.

2.2 Rede Ethereum

Dentre as diversas redes blockchain, a rede *Ethereum* foi criada por Vitalik Buterin em 2014, com o objetivo de oferecer uma plataforma descentralizada e *Turing-complete* para o de-

envolvimento de aplicações digitais. Por ser *Turing-complete*, o *Ethereum* permite a execução de processos computacionais complexos, o que possibilita a criação de contratos inteligentes (*smart contracts*) e a implantação de aplicações descentralizadas (*DApps*). E, além dessa flexibilidade, essa rede destaca-se pela capacidade de realizar transações envolvendo diferentes tipos de ativos digitais, o que amplia suas possibilidades de aplicação em diversos setores [Buterin, 2014].

Os contratos inteligentes, elementos centrais da arquitetura do *Ethereum*, são protocolos computacionais autoexecutáveis responsáveis por implementar regras de negócio e lógicas operacionais diretamente na rede blockchain. Eles automatizam a execução de condições pré-estabelecidas sem a necessidade de intervenção humana ou de uma autoridade central. Já as *DApps* são aplicações que, diferentemente de softwares tradicionais, não estão hospedadas em um único servidor, mas sim distribuídas entre os nós da rede. E ao interagir com uma *DApp*, os usuários estão executando operações que disparam chamadas aos contratos inteligentes, o que garante descentralização e resistência a censura [Buterin, 2014].

Além da execução de lógicas complexas, a rede consolidou padrões de interoperabilidade para a criação de ativos digitais, sendo o ERC-20 (*Ethereum Request for Comments 20*) o mais difundido. Este padrão estabelece uma interface comum para a criação de tokens fungíveis, ativos que são idênticos entre si e podem ser trocados na mesma proporção. Ao definir regras estritas de implementação, como métodos de transferência e consulta de saldo, o padrão ERC-20 permite que diferentes aplicações, carteiras e corretoras interajam com novos ativos de forma previsível e segura, fomentando o crescimento do ecossistema de finanças descentralizadas e economias digitais.

No contexto de execução, a *Ethereum Virtual Machine (EVM)* representa o ambiente computacional que permite a implementação e a execução de contratos inteligentes e *DApps*. Essa infraestrutura atua como uma camada de abstração que isola e executa as instruções dos contratos de maneira segura e distribuída. E, além do mais, os recursos computacionais consumidos durante essas operações são regulados por meio de um sistema de taxas (*gas*), que estabelece limites para o processamento de cada transação, garantindo a equidade no uso da rede e a proteção contra abusos e ataques de negação de serviço.

2.3 Redes EVM-Compatible

As redes *EVM-Compatible* representam uma evolução no ecossistema blockchain ao oferecer um ambiente de execução compatível com a *Ethereum Virtual Machine (EVM)*. Essa característica permite que contratos inteligentes desenvolvidos para a rede *Ethereum* sejam implantados em outras redes sem modificações, garantindo portabilidade de *DApps* e continuidade no uso de linguagens e ferramentas já consolidadas, como a linguagem de programação *Solidity* e o *framework Ethers.js* [Jia and Yin, 2022].

A principal vantagem dessas redes está na redução significativa dos custos de transação e na maior rapidez na confirmação de blocos, quando comparadas à rede *Ethereum*. Em 07/09/2025, o token nativo ETH estava cotado em aproximadamente US\$ 4.291,79, resultando em taxas médias entre US\$ 2,50 e US\$ 5,00 para uma simples transferência de tokens ERC-20. Em contraste, a mesma operação em redes como *Polygon* (POL a US\$ 0,28) ou *Avalanche* (AVAX a US\$ 24,50) pode custar até 500 vezes menos, situando-se na faixa de US\$ 0,005 a US\$ 0,01 por transação. Essa diferença torna o uso de contratos inteligentes muito mais acessível, especialmente em cenários de alta demanda ou aplicações que exigem grande volume de operações.

Nesse contexto, as redes *EVM-Compatible* se consolidam como uma alternativa estratégica para projetos que buscam escalabilidade, redução de custos e manutenção da compatibilidade com o ecossistema *Ethereum*. Essa combinação favorece a adoção em larga escala de aplicações descentralizadas, soluções corporativas e iniciativas em *DeFi*, tornando-as uma base sólida para o desenvolvimento de novos sistemas blockchain.

2.4 Carteiras de usuário e padrões de conectividade em aplicações descentralizadas

Em blockchain, uma carteira de usuário (*wallet*) é um componente fundamental que armazena as chaves criptográficas dos usuários: a chave privada, que é usada para assinar e autorizar transações, e a chave pública, que gera o endereço visível na rede. Essas carteiras não armazenam os ativos em si, mas controlam os direitos de movimentação e de acesso aos saldos registrados na blockchain. Sem uma carteira, não seria possível comprovar propriedade, enviar ou receber ativos, ou interagir com contratos inteligentes.

O conceito de interface de carteira (*interface wallet*) é uma das ferramentas mais populares

do ecossistema de aplicações descentralizadas, geralmente disponível como extensão de navegador ou aplicativo móvel. Essa ferramenta visa simplificar a experiência do usuário ao gerar automaticamente as credenciais criptográficas e fornecer um mecanismo de recuperação seguro, como a frase-semente (*seed phrase*). Quando um usuário acessa uma aplicação descentralizada, o sistema solicita conexão com a interface de carteira, que retorna apenas o endereço público do usuário, garantindo que a chave privada jamais seja exposta. Toda transação ou ação que altera o estado da rede só pode ser autorizada após confirmação manual do usuário na interface da carteira, o que assegura segurança e transparência no processo de autenticação e autorização de ações [Sultana et al., 2023].

Além de facilitar o uso de aplicações descentralizadas, a interface de carteira ajuda estabelecer padrões amplamente adotados nesse ecossistema, como o uso do protocolo *JSON-RPC* e os métodos específicos de solicitação de conta, como o *eth_requestAccounts*, para autenticação. A universalidade desses padrões permitiu que diferentes carteiras se tornassem interoperáveis com as mesmas interfaces de aplicações descentralizadas. Dessa forma, a carteira evoluiu para ser um elemento central na segurança, privacidade e identidade auto-soberana do usuário, onde o controle de credenciais reside inteiramente com o indivíduo, reforçando a descentralização dos sistemas baseados em blockchain [MetaMask, 2025].

2.5 Processamento em lote

O processamento em lote (*batch processing*) caracteriza-se como um modelo em que grandes volumes de dados são preparados e executados de forma automatizada, sem a necessidade de interação manual constante. Historicamente, essas operações são estruturadas para maximizar a utilização dos recursos de infraestrutura, permitindo que o sistema processe tarefas sequencialmente e explore períodos de menor carga computacional para otimizar o rendimento (*throughput*) global [Silberschatz et al., 2018]. Essa característica torna o modelo especialmente adequado para cenários em que a escalabilidade e a otimização de custos operacionais são requisitos fundamentais.

A minimização da interação humana nesse processo, além de reduzir o tempo gasto em tarefas repetitivas, também diminui significativamente a probabilidade de erros operacionais derivados de entradas manuais. Em sistemas modernos, o gerenciamento desses fluxos é realizado por plataformas de orquestração que garantem a atomicidade das operações e a rastreabilidade das tarefas. Tais ferramentas permitem a detecção automática de falhas e a implementação

de políticas de recuperação, assegurando que o processamento de grandes conjuntos de dados ocorra de maneira resiliente e eficiente [Tanenbaum and Bos, 2015].

Aplicada ao contexto deste trabalho, a arquitetura *batch* garante o processamento eficiente de grandes volumes de dados acadêmicos antes de sua inserção na blockchain. Esse modelo é especialmente útil no encerramento dos períodos letivos, quando há maior concentração de registros a serem atualizados. Dessa forma, a etapa de ingestão em lote permite consolidar informações como cursos, disciplinas e notas em pacotes estruturados, que posteriormente são submetidos à blockchain de maneira otimizada. Essa estratégia não apenas reduz custos associados a múltiplas transações individuais, mas também preserva a imutabilidade e a segurança dos registros, conciliando eficiência operacional com a confiabilidade exigida em ambientes educacionais descentralizados.

2.6 Criptografia aplicada à proteção de dados

A criptografia constitui a base fundamental para a segurança da informação em ambientes digitais, atuando na transformação de dados legíveis em conteúdos cifrados, acessíveis apenas a portadores de credenciais autorizadas. Essa técnica é essencial para mitigar riscos de acesso indevido ou manipulação de dados, oferecendo garantias robustas de confidencialidade, integridade e autenticidade [Stallings, 2017]. No contexto de sistemas descentralizados, a eficácia da proteção depende não apenas da robustez dos algoritmos, mas também de uma gestão de chaves eficiente e segura.

Os modelos de criptografia dividem-se em simétricos e assimétricos. A criptografia simétrica utiliza uma única chave compartilhada para as operações de cifragem e decifragem, destacando-se pela eficiência no processamento de grandes volumes de dados. O algoritmo Advanced Encryption Standard (AES) consolidou-se como o padrão desta categoria, operando em blocos de 128 bits [National Institute of Standards and Technology, 2001]. Para assegurar a variabilidade estatística e impedir a identificação de padrões em dados repetitivos, utiliza-se um Initialization Vector (IV), um valor aleatório que garante que a mesma informação, quando cifrada repetidamente com a mesma chave, resulte em textos cifrados distintos [Stallings, 2017].

A criptografia assimétrica, por sua vez, baseia-se em um par de chaves correlacionadas: uma pública, destinada à cifragem, e uma privada, mantida sob sigilo para a decifragem. Este modelo elimina a necessidade de compartilhamento prévio de segredos, sendo exemplificado pelo esquema Elliptic Curve Integrated Encryption Scheme (ECIES). Ele combina a eficiência da

cifragem simétrica com a segurança da criptografia de curva elíptica, utilizando padrões como a curva *secp256k1*, amplamente adotada em redes blockchain devido ao seu equilíbrio entre desempenho computacional e segurança criptográfica [Flavius, 2022]. Complementarmente, o algoritmo Elliptic Curve Digital Signature Algorithm (ECDSA) é empregado para assinaturas digitais sobre funções de *hash* como o *Keccak-256*, assegurando a proveniência e a imutabilidade das mensagens assinadas.

Um desafio crítico na implementação de sistemas criptográficos é a proteção das chaves privadas dos usuários. Para evitar o armazenamento de chaves em texto simples ou a dependência exclusiva de dispositivos físicos, utiliza-se a derivação de chaves baseada em senhas (*Password-Based Cryptography*). Neste cenário, destaca-se o algoritmo Password-Based Key Derivation Function 2 (PBKDF2), que aplica uma função pseudoaleatória a uma senha mestra fornecida pelo usuário, combinada a um *salt*, um dado aleatório que impede ataques de dicionário e tabelas de consulta pré-computadas. Através de um elevado número de iterações, o PBKDF2 deriva uma chave de alta entropia, que é então utilizada pelo AES para cifrar a chave privada do usuário, criando uma camada de proteção conhecida como *keystore*. Essa abordagem permite que segredos criptográficos complexos sejam protegidos por senhas humanas, garantindo que o acesso aos dados sensíveis e a capacidade de assinatura digital permaneçam sob o controle exclusivo e soberano do utilizador.

2.7 Gestão de identidade e controle de acesso em ambientes distribuídos

A gestão de identidade em sistemas distribuídos apresenta desafios distintos dos modelos tradicionais centralizados, exigindo uma transição de repositórios de dados unificados para mecanismos baseados em credenciais criptográficas soberanas. Em ambientes descentralizados, a identidade de cada participante é representada por um par de chaves assimétricas, onde a chave pública atua como um identificador único e verificável na rede, enquanto a chave privada é a ferramenta de validação de transações e interações. Esta arquitetura elimina a dependência de autoridades centrais, mas transfere ao usuário a responsabilidade crítica pela custódia de suas chaves. Para viabilizar essa autonomia de forma segura para usuários não técnicos, a gestão de identidade moderna incorpora camadas de proteção local, como o uso de funções de derivação de chave (PBKDF2) para cifrar chaves privadas sob senhas mestras, garantindo que a soberania digital não resulte em vulnerabilidade por perda ou exposição de segredos.

Dentro desse contexto, o controle de acesso deixa de ser uma função exercida por adminis-

tradadores de sistema e passa a ser um atributo intrínseco aos dados e às permissões criptográficas. Modelos comuns de controle de acesso perdem aplicabilidade em redes abertas, sendo substituídos por protocolos de compartilhamento condicional baseados em criptografia assimétrica. No modelo de registros acadêmicos distribuídos, o acesso a informações sensíveis é gerido diretamente pelo proprietário do dado, o estudante, que utiliza a chave pública de terceiros interessados para recifrar informações via ECIES. Esse processo permite definir políticas de acesso granulares e dinâmicas, onde a autorização não é apenas um registro lógico em um banco de dados, mas uma impossibilidade matemática de acesso para quem não possui a chave privada correspondente.

A imutabilidade e a transparência da blockchain complementam esse cenário ao fornecer rastreabilidade e auditabilidade plena às ações de controle de acesso. A combinação de algoritmos de assinatura digital, como o ECDSA, com funções de *hash* criptográfico, como o *Keccak-256*, permite verificar a autoria e a integridade de cada registro acadêmico e de cada concessão de acesso sem a necessidade de intermediários. Ao unir a eficiência da cifragem simétrica para o armazenamento de grandes volumes de dados com a segurança da criptografia assimétrica para a distribuição de chaves, esses sistemas estabelecem um ambiente de confiança mútua. O resultado é uma infraestrutura de identidade descentralizada onde a privacidade é preservada pela criptografia e a legitimidade é assegurada pelo consenso da rede, devolvendo ao estudante o controle sobre seu histórico e sua vida acadêmica.

Capítulo 3

Trabalhos relacionados

Pesquisas recentes têm explorado o uso da tecnologia blockchain para aprimorar a gestão de registros acadêmicos. Este capítulo apresenta e analisa os principais trabalhos existentes na literatura que abordam a descentralização desses registros, buscando identificar contribuições relevantes e lacunas ainda presentes.

Para essa análise, foi realizada uma busca na base de dados do IEEE e Google Scholar utilizando os termos "*blockchain*", "*higher education*" e "*academic registry*", com o objetivo de localizar estudos voltados à aplicação prática da tecnologia no setor educacional. Os trabalhos selecionados incluem tanto propostas conceituais quanto experimentos de implementação em ambientes acadêmicos reais, sendo de particular interesse aqueles que oferecem soluções próximas à realidade das instituições. E com essa revisão, foi possível entender melhor o cenário atual e mostrar como a proposta deste trabalho se diferencia das soluções já existentes.

A revisão realizada por [P et al. \[2023\]](#) evidencia que a aplicação de blockchain no âmbito educacional vai muito além da simples emissão de diplomas digitais, englobando desde o registro de credenciais acadêmicas até sistemas de tutoria adaptativa e financiamento estudantil. Os autores identificam casos de uso onde a imutabilidade da cadeia de blocos garante rastreabilidade e confiança em registros de aprendizagem ao longo do tempo, permitindo que plataformas de gestão de aprendizagem (LMS) ajustem conteúdos de forma personalizada conforme o progresso do aluno. Nesse sentido, um sistema descentralizado de registros acadêmicos poderia empregar contratos inteligentes para acumular crédito sempre que uma disciplina é concluída, assegurando que cada evento seja atestado dentro da blockchain por instituições autorizadas.

Entretanto, a mesma revisão destaca desafios técnicos significativos para a adoção em larga escala, em especial a escalabilidade das redes blockchain públicas, cujo aumento de transações pode elevar custos de taxas (*gas*) e provocar gargalos. Para resolver essas limitações, [P et al.](#) sugerem o uso de algoritmos de consenso mais leves, como *Proof of Stake*, e arquiteturas externas ou suplementares a blockchain que aliviem parte do processamento crítico da camada principal. Em um protótipo *EVM-Compatible*, essa estratégia poderia se traduzir na implementação sobre uma solução *Layer-2*, como *Polygon* ou *Optimism*, de modo a manter a imutabilidade dos re-

gistros sem comprometer a eficiência e a viabilidade econômica do sistema.

Em relação à privacidade e ao controle de acesso, a revisão aponta a necessidade de técnicas avançadas como criptografia, provas de conhecimento zero e armazenamento de documentos em InterPlanetary File System (IPFS) com apenas seus *hashes* registrados dentro da blockchain. Essa combinação garante que informações sensíveis permaneçam criptografadas e acessíveis somente a usuários autorizados, enquanto a rede conserva um registro auditável de todas as transações. Assim, nosso projeto proposto para registros descentralizados considerará alguns desses mecanismos para prover confidencialidade e conformidade com regulamentações como a Lei Geral de Proteção de Dados (LGPD).

Um outro trabalho relacionado à temática abordada neste trabalho é o proposto por [Mali et al. \[2023\]](#), que apresenta um sistema de gerenciamento de créditos acadêmicos baseado em blockchain, alinhado às diretrizes da *University Grants Commission* (UGC) da Índia. Nesse artigo, os autores propõem uma plataforma pública na qual diferentes instituições de ensino superior atuam como nós de uma rede blockchain, possibilitando o armazenamento imutável e transparente de históricos acadêmicos e dados pessoais dos estudantes. Essa proposta busca solucionar ineficiências do modelo tradicional, oferecendo aos alunos maior controle sobre seus próprios registros acadêmicos, por meio de uma interface descentralizada, segura e auditável.

A solução desenvolvida também incorpora contratos inteligentes (*smart contracts*) para automatizar processos administrativos, como matrícula, alocação de créditos e emissão de certificados. O sistema permite que os estudantes consultem um catálogo de cursos, realizem inscrições e acompanhem o progresso acadêmico por meio de painéis personalizados. Os créditos acumulados e os certificados obtidos são verificados por uma autoridade central e registrados permanentemente na blockchain, promovendo uma experiência educacional mais fluida e confiável entre instituições [[Mali et al., 2023](#)].

Esse trabalho oferece informações valiosas sobre o potencial da tecnologia blockchain para transformar a gestão de registros acadêmicos e validações de créditos, servindo como referência direta para o desenvolvimento do presente trabalho, que também explora a utilização da blockchain no contexto educacional, embora com objetivos e arquitetura distintos.

Outro trabalho que servirá como base para o desenvolvimento deste projeto é o de [Pedrosa et al. \[2025\]](#), que apresenta uma prova de conceito de um sistema de registros acadêmicos baseado em blockchain, implementado na rede *Ethereum*. Nessa solução, os registros acadêmicos são armazenados na blockchain e inseridos por meio de uma interface web desenvolvida especi-

ficamente para essa finalidade. O principal objetivo do sistema é garantir que os alunos tenham acesso aos seus históricos escolares, mesmo em casos de falhas institucionais, evitando a perda ou indisponibilidade de documentos importantes.

A proposta busca fortalecer a segurança e a integridade dos dados acadêmicos, ampliando as garantias fornecidas pelos sistemas tradicionais. Por meio da utilização de contratos inteligentes, o sistema permite a inserção de instituições, cursos, disciplinas, alunos e suas respectivas notas de forma transparente e auditável [Pedrosa et al., 2025]. Essa abordagem representa um avanço no controle e na rastreabilidade dos registros educacionais, demonstrando o potencial da tecnologia blockchain no contexto acadêmico.

Por fim, o sistema descrito por Pedrosa et al. [2025] torna-se o principal motivador para a realização deste trabalho, oferecendo uma base concreta que demonstra, de forma prática, tanto os benefícios quanto os desafios de migrar para uma arquitetura descentralizada. Embora apresente algumas limitações, sua implementação inicial evidencia um caminho promissor para a modernização dos processos de gestão acadêmica, servindo como ponto de partida para as melhorias propostas neste trabalho.

Kistaubayev et al. [2023] apresenta o desenvolvimento e a avaliação da plataforma *UniverCert*, uma solução baseada em blockchain voltada para a criação de registros digitais das atividades acadêmicas de estudantes do ensino superior. O principal objetivo do sistema é resolver problemas como fraudes e falsificações em registros acadêmicos, além de promover a descentralização e a segurança no armazenamento desses dados. Por meio dessa abordagem, o *UniverCert* busca garantir a integridade e a autenticidade das informações educacionais, respondendo a uma necessidade crescente por maior confiabilidade nos processos de gestão acadêmica.

Para atingir esses objetivos, Kistaubayev et al. [2023] adotaram uma arquitetura híbrida composta por uma camada fora e outra dentro da blockchain. A camada fora da blockchain é responsável por armazenar dados mais volumosos e detalhados, como nomes de alunos e descrições de cursos, utilizando um banco de dados tradicional. Já a camada dentro da blockchain concentra as informações mais críticas, como registros de conclusão de disciplinas e notas, armazenadas de forma compacta por meio de IDs e valores numéricos. Essa parte do sistema foi implementada em uma blockchain permissionada baseada no *Ethereum*, onde apenas nós previamente autorizados têm permissão para validar transações, o que garante maior rapidez na execução das operações e redução significativa nos custos relacionados ao consumo de *gas*.

[Kistaubayev et al., 2023].

Além disso, o Kistaubayev et al. [2023] incorpora uma camada intermediária de comunicação por meio de uma *API REST*, responsável pela autenticação dos usuários, controle de acesso, gerenciamento das transações com o banco de dados relacional e ativação dos contratos inteligentes. A avaliação experimental realizada pelos autores demonstrou que a arquitetura híbrida proporciona baixos custos de transação, com tempo médio de confirmação de cerca de 4,2 segundos e utilização eficiente de espaço, com menos de 1 KB por registro semestral. Essas características evidenciam a viabilidade da solução para cenários de grande escala. O *UniverCert* apresenta conceitos e estratégias que dialogam diretamente com os objetivos deste trabalho, especialmente no que diz respeito à redução de custos, à eficiência na gestão de dados acadêmicos e à integração entre camadas externas e internas à blockchain conforme é mostrado na Figura 2.

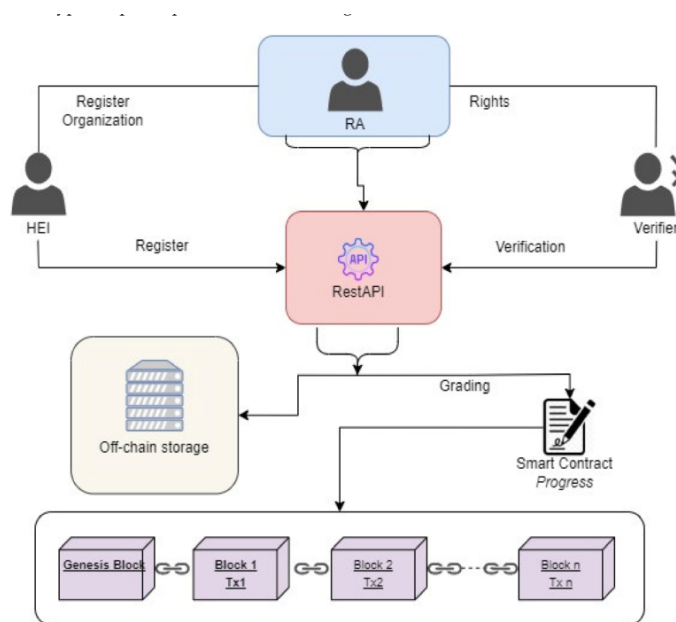


Figura 2: Arquitetura do UniverCert [Kistaubayev et al., 2023]

Tabela 1: Síntese crítica dos trabalhos relacionados

Estudo	Contribuições	Limitações	Como nosso artigo avança
Pedrosa et al. (2025)	Prova de conceito na blockchain com contratos em <i>Solidity</i> e interface em <i>React</i> . Mostrou viabilidade e rastreabilidade.	Alto custo de <i>gas</i> , baixa usabilidade, dependência de funções depreciadas do <i>MetaMask</i> .	Introduz ingestão em lote fora da blockchain, criptografia híbrida sem <i>MetaMask</i> , carteiras embarcadas e redes <i>EVM-Compatible</i> .
Kistaubayev et al. (2023)	Arquitetura híbrida (dados fora da blockchain, <i>hashes</i> dentro da blockchain) com bons resultados de custo e latência.	Uso de blockchain permissionada (menos descentralização), pouco foco em <i>onboarding</i> de usuários.	Adota blockchain pública <i>EVM-Compatible</i> com criptografia avançada (PBKDF2 + AES + ECIES), garantindo interoperabilidade e privacidade.
Mali et al. (2023)	Integração institucional e automação de políticas via contratos inteligentes.	Dependência de autoridade central e ausência de otimização de custos para inserções em massa.	Propõe compartilhamento controlado pelo aluno e ingestão em lote para reduzir custos.
P et al. (2023)	Identifica tendências (camadas fora da blockchain, ZKPs, IPFS) e principais desafios (escalabilidade, privacidade).	Não avalia <i>trade-offs</i> práticos nem fornece métricas experimentais.	Realiza experimentos empíricos de custo e desempenho entre <i>Ethereum</i> e redes <i>EVM-Compatible</i> .

A Tabela 1 apresenta uma síntese crítica dos trabalhos analisados, destacando as principais contribuições, limitações e a forma como este trabalho avança em relação a cada um deles. Observa-se que as pesquisas recentes comprovam a viabilidade da utilização de blockchain para a gestão de registros acadêmicos, porém ainda enfrentam barreiras técnicas e operacionais que dificultam sua adoção em larga escala. Enquanto propostas como a de [Pedrosa et al. \[2025\]](#) reforçam o potencial da rastreabilidade e transparência de sistemas totalmente dentro da blockchain, seu alto custo de *gas* e a baixa usabilidade limitam a aplicabilidade prática. Já abordagens híbridas, como a de [Kistaubayev et al. \[2023\]](#), conseguem mitigar custos e latência, mas sacrificam parte da descentralização ao recorrer a uma blockchain permissionada.

Outros trabalhos, como o de [Mali et al. \[2023\]](#), destacam a integração institucional e a automação de processos por meio de contratos inteligentes, mas ainda dependem de autoridades centrais e não exploram estratégias de otimização de inserções em massa. Revisões mais amplas, como a de [P et al. \[2023\]](#), oferecem um panorama valioso sobre tendências emergentes mas carecem de análises empíricas sobre *trade-offs* práticos.

Diante desse cenário, o trabalho aqui proposto busca avançar em quatro dimensões principais: adoção de redes públicas *EVM-Compatible* que conciliam eficiência e redução de custos, introdução de estratégias de ingestão em lote, criptografia híbrida para aumentar a privacidade, e carteiras embarcadas para garantir um modelo de compartilhamento seguro e acessível. Assim, nossa proposta se diferencia por alinhar eficiência, interoperabilidade e conformidade regulatória, superando limitações recorrentes nos estudos analisados e oferecendo um caminho mais robusto e escalável para a descentralização de registros acadêmicos.

Capítulo 4

Desenvolvimento

4.1 Cenário de negócio e processos acadêmicos

A gestão de registros acadêmicos não é apenas um desafio tecnológico, mas um processo de negócio crítico que envolve a custódia de ativos e a garantia de continuidade da trajetória profissional dos estudantes. No modelo tradicional centralizado, as instituições de ensino atuam como as únicas guardiãs de um acervo documental que deve, por lei, ser preservado permanentemente. Contudo, como demonstrado pelo histórico de descredenciamento de instituições, a falência ou o encerramento das atividades de uma universidade interrompe o fluxo de negócio, impossibilitando que o ex-aluno obtenha provas de sua formação para o mercado de trabalho ou para a continuidade de estudos em outras instituições.

Dentro deste ecossistema, identificam-se três atores principais cujas interações definem o fluxo de valor do sistema. A instituição de ensino atua como a autoridade emissora; seu papel de negócio é assegurar a integridade e a autenticidade dos cursos, disciplinas e notas lançadas. Para a instituição, a adoção de uma solução descentralizada representa uma redução de custos operacionais com secretarias e uma mitigação de riscos jurídicos relacionados à perda de dados. O estudante, por sua vez, assume o papel de proprietário soberano de seus dados. Em vez de ser um usuário passivo de um banco de dados institucional, ele detém as chaves de acesso que permitem a portabilidade de seu histórico, facilitando processos de transferência e mobilidade acadêmica.

A figura do visitante (empresas em processos de contratação ou outras universidades) representa o ponto de consumo dos dados. No cenário atual, a validação de um diploma é um processo burocrático que pode levar semanas, envolvendo trocas de e-mails e telefonemas entre departamentos de recursos humanos e secretarias acadêmicas. Com a solução proposta, este processo de negócio é transformado em uma verificação instantânea e automatizada, onde o visitante solicita acesso e o estudante concede a visualização de forma imediata e auditável.

Por fim, a viabilidade deste modelo de negócio depende da escalabilidade administrativa. Processos acadêmicos reais operam em picos sazonais, como o fechamento de períodos letivos,

onde milhares de notas precisam ser homologadas simultaneamente. Portanto, a transição para um sistema em blockchain exige que as operações não apenas sejam seguras, mas que suportem o volume operacional de uma secretaria acadêmica sem gerar gargalos financeiros ou de tempo. A solução aqui desenvolvida busca, portanto, traduzir essas necessidades do mundo real em uma arquitetura que equilibra a confiança da descentralização com a eficiência necessária para a prática cotidiana das instituições de ensino. Com foco na transformação dos processos acadêmicos, este trabalho baseia-se inicialmente na solução de [Pedrosa et al. \[2025\]](#), apresentada em detalhes a seguir.

4.2 O sistema-base da prova de conceito

O trabalho desenvolvido por [Pedrosa et al. \[2025\]](#) apresenta uma prova de conceito de um sistema para gestão de registros acadêmicos utilizando a tecnologia blockchain. E, como já apontado, a motivação para o estudo surgiu a partir de casos reais no Rio de Janeiro, como o credenciamento das universidades *Gama Filho* e *UniverCidade* em 2014, que resultou na dificuldade de ex-alunos acessarem seus diplomas e históricos, pois os documentos físicos ficaram sob a guarda dos representantes legais das instituições [[Bom Dia Rio, 2019](#)]. A essência da solução está na implementação de um contrato inteligente escrito com a linguagem de programação *Solidity*, implantado na rede *Ethereum*, que centraliza as regras de armazenamento de registros acadêmicos. Para assegurar a autenticidade dos participantes, as instituições de ensino devem registrar suas chaves públicas dentro da blockchain, criando um repositório acadêmico descentralizado, seguro e imutável. Essa abordagem busca resolver riscos típicos dos modelos centralizados, como a perda ou a manipulação indevida de registros.

A modelagem conceitual do sistema é representada pelo diagrama de classes da Figura 3, a partir do qual foram definidas as entidades e suas relações. A entidade *Institution* representa a instituição de ensino, identificada por seu endereço na blockchain e nome, sendo responsável por registrar alunos, cursos, disciplinas e notas. O *Student* representa o aluno, cujos dados pessoais sensíveis são criptografados para garantir a privacidade em conformidade com a LGPD. Já o *Course* define o curso, com atributos como código, nome, tipo (Bacharelado, Mestrado, etc.) e número de semestres, enquanto a entidade *Discipline* organiza as disciplinas, incluindo código, nome, ementa, carga horária e créditos. Por fim, a entidade *Grade* registra as informações referentes a uma disciplina cursada por um aluno, como nota, ano, semestre e status de aprovação.

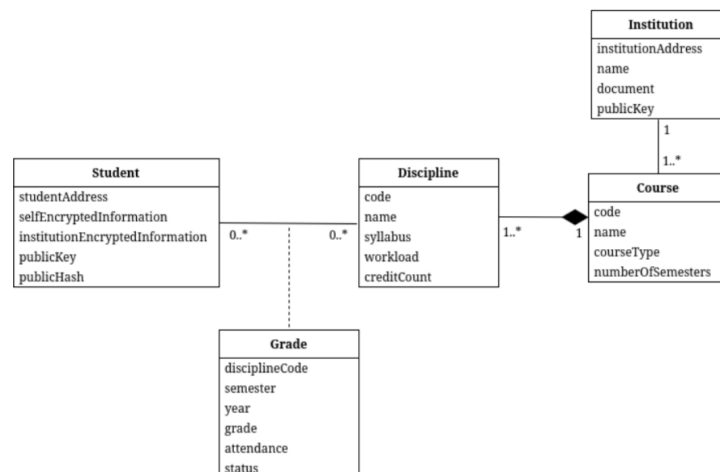


Figura 3: Diagrama de classes de Pedrosa et al. [2025]

Tabela 2: Tabela dos requisitos funcionais

Identificador	Requisito	Ator	Precedente
RF01	Registrar instituições	Dono do contrato	-
RF02	Compartilhar chave pública	Instituição	RF01
RF03	Cadastrar curso	Instituição	RF01
RF04	Cadastrar disciplina	Instituição	RF03
RF05	Cadastrar registro de aluno	Instituição	RF01
RF06	Cadastrar nota do aluno	Instituição	RF04, RF05
RF07	Cadastrar informações pessoais do aluno	Aluno	RF02, RF05
RF08	Confirmar informações pessoais do aluno	Instituição	RF07
RF09	Solicitar acesso aos dados do aluno	Solicitante	-
RF10	Gerir autorização de acesso aos dados	Aluno	RF08, RF09
RF11	Consultar histórico do aluno	Aluno, Instituição, Autorizados	RF08 e RF10

O sistema oferece um conjunto de operações que incluem desde o cadastro das instituições de ensino até a visualização dos históricos escolares pelos alunos ou por terceiros autorizados.

Entre as principais funções estão: o registro de instituições (RF01), o compartilhamento das chaves públicas de encriptação das instituições (RF02), o cadastro de cursos (RF03) e disciplinas (RF04), e o registro de alunos (RF05). Além disso, é possível incluir notas (RF06), bem como permitir que os próprios alunos insiram e confirmem suas informações pessoais (RF07 e RF08). Outro diferencial importante é o processo de gestão de permissões: um terceiro interessado pode solicitar acesso aos dados de um aluno (RF09), e cabe ao próprio aluno conceder ou negar essa autorização (RF10). Tanto o aluno, quanto a instituição ou usuários autorizados podem consultar os históricos e os dados pessoais (RF11). Essas interações estão bem sintetizadas na Tabela 2 do trabalho original, que lista todos os requisitos funcionais do sistema.

Um aspecto técnico relevante do sistema-base é a sua dependência da emissão de eventos (*Events*) no contrato inteligente para a persistência de *logs* de auditoria. No modelo de Pedrosa et al. [2025], os eventos funcionam como um registro histórico imutável das ações administrativas, permitindo que a interface recupere a trajetória de um aluno sem sobrecarregar o estado global da rede. Além disso, o fluxo de gestão de permissões (RF09 e RF10) estabelece uma barreira de segurança onde o dado nunca é exposto sem uma interação transacional direta do estudante, consolidando o conceito de soberania de dados, embora isso implique em uma dependência operacional de o aluno estar presente para processar cada pedido de acesso.

Para viabilizar essas funcionalidades, a interface de usuário do sistema foi desenvolvida utilizando o *framework React*, com a comunicação com o contrato inteligente sendo feita por meio da biblioteca *Ethers.js*. Toda interação transacional requer a assinatura de transações via a interface de carteira *MetaMask*, criando um fluxo que introduz um alto grau de complexidade e dependência para o usuário final. Cada inserção ou alteração de dados demanda múltiplas etapas de confirmação de transações e ajustes manuais de parâmetros como o *gas limit*. Essas exigências técnicas podem comprometer a experiência do usuário, especialmente para públicos com menor familiaridade com ferramentas *Web3*.

Embora a prova de conceito tenha demonstrado a viabilidade técnica da proposta, é importante reconhecer que ela representa uma solução inicial, com foco principal em validar a aplicabilidade da tecnologia blockchain no contexto acadêmico. Desse modo, o sistema serviu como um ponto de partida significativo para novas pesquisas e desenvolvimentos, incluindo este trabalho, que busca aprimorar a proposta original, adequando sua arquitetura a cenários de maior escala e usabilidade.

4.3 Limitações do sistema-base

Apesar de seu caráter inovador e de sua contribuição relevante para a área, o sistema-base apresenta algumas limitações que se tornam evidentes quando se considera a adoção da solução em um ambiente educacional real e de larga escala. Essas fragilidades não invalidam os méritos da proposta original, mas evidenciam aspectos que necessitam de aprimoramentos para viabilizar uma implementação prática e eficiente, sendo elas:

Operações manuais excessivas. O sistema original exige que cada usuário conecte sua carteira e assine manualmente cada transação de inclusão de dado, seja o cadastro de um curso, a matrícula de um aluno ou o lançamento de uma nota. Esse fluxo torna-se rapidamente impraticável sempre que há necessidade de inserir grandes volumes de registros, consumindo tempo e aumentando a chance de erros humanos. Além disso, a repetição de interações de confirmação e ajustes constantes de parâmetros de taxa comprometem a fluidez do processo e afasta usuários menos familiarizados com as peculiaridades de transações em blockchain.

Dependência de biblioteca obsoleta do *MetaMask*. A criptografia de dados pessoais dos estudantes em cada nova operação depende da função *eth_getEncryptionPublicKey*, fornecida pela biblioteca *@metamask/eth-sig-util*, atualmente considerada obsoleta. A principal razão para essa descontinuação foi uma preocupação de segurança relacionada ao fato de que a mesma chave privada utilizada para assinar transações também era empregada para operações de cifragem, contrariando boas práticas de criptografia. Esse modelo aumenta significativamente o risco de exposição da chave privada e viola o princípio da separação entre funções criptográficas distintas [MetaMask Team, 2023]. Portanto, a falta de uma alternativa consolidada para essa função de encriptação reforça a fragilidade da solução-base e aponta para a necessidade de um método diferente e desacoplado de serviços terceiros específicos.

Alto custo em taxas (*gas*). Uma vez que toda operação de gravação é registrada na rede *Ethereum*, as taxas associadas a essas operações somam valores consideráveis, especialmente em momentos de grande volume de transações na rede. Instituições que precisem atualizar periodicamente milhares de registros de alunos veriam seus custos operacionais aumentarem de forma não linear, limitando a adoção do sistema e gerando barreiras financeiras para usuários finais. Dessa forma, esse fator econômico desfavorece não só testes em ambientes reais, mas também quaisquer cenários de uso em larga escala, em que menores instituições ou pequenos centros de extensão não possam arcar com as despesas elevadas.

Escalabilidade comprometida. Sem qualquer camada fora da blockchain para agregação ou pré-processamento de dados, cada novo registro amplia diretamente o estado do contrato inteligente, elevando a complexidade e o tempo de leitura e escrita conforme o volume cresce. Conforme mapeamentos na blockchain se tornam mais extensos, operações passam a demandar mais taxas (*gas*). A ausência de mecanismos de processamento em lote impede o sistema-base de suportar cargas elevadas de forma eficiente, reduzindo sua viabilidade em instituições de grande porte ou em ambientes que requerem atualizações contínuas de informações.

Baixa usabilidade. Para interagir com a aplicação descentralizada, o usuário precisa instalar e configurar manualmente uma extensão de interface de carteira *MetaMask*, selecionar redes compatíveis, gerenciar endereços e chaves, o que impõe uma curva de aprendizado elevada. Esse nível de complexidade alia-se à necessidade de conhecimentos técnicos sobre *Ethereum* e bibliotecas *Web3*, afastando grande parte do público acadêmico, especialmente estudantes e professores sem conhecimento prévio em blockchain. Como resultado, a solução-base carece de uma interface mais acessível, limitando seu potencial de adoção.

4.4 Concepção da solução

Com base na análise das limitações identificadas no sistema-base, este trabalho propõe uma nova arquitetura que visa elevar a viabilidade técnica e operacional da gestão de registros acadêmicos. O objetivo central é superar os obstáculos de escalabilidade e experiência do usuário, estabelecendo um modelo de confidencialidade seletiva. Nesta abordagem, a transparência da blockchain é utilizada para o registro público de dados curriculares e avaliativos, enquanto a criptografia robusta é reservada estritamente para a proteção da identidade dos estudantes, garantindo conformidade com normas de privacidade e eficiência de custos.

A arquitetura do sistema é estruturada em três domínios principais: a interface de usuário (UI), a camada de serviço e a camada de consenso, conforme ilustrado na Figura 4. Enquanto a camada de consenso garante a imutabilidade global, a camada de serviço atua como um acelerador operacional de responsabilidade da instituição. Este domínio introduz um componente de orquestração e processamento em lote que automatiza a ingestão de registros. Embora essa camada introduza um componente centralizado na arquitetura, sua função é estritamente de preparação e otimização; a validade jurídica e a perenidade dos dados permanecem dependentes apenas da camada de consenso após a publicação. Esse fluxo elimina a necessidade de submissões manuais e individuais, permitindo que grandes volumes de dados acadêmicos sejam

enviados à rede em operações únicas de *batching*, otimizando o uso de *gas* e o tempo administrativo.

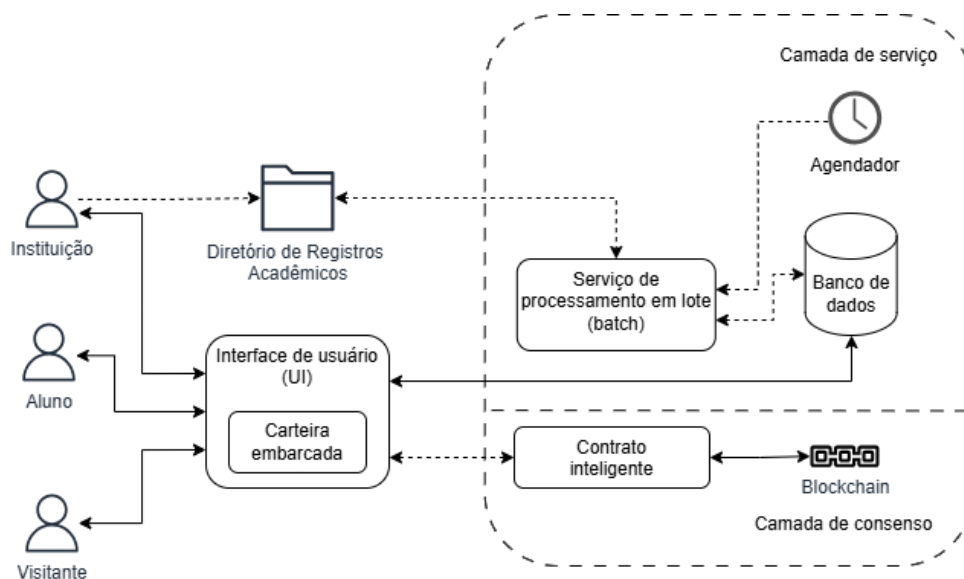


Figura 4: Arquitetura geral do sistema descentralizado de registro acadêmico

A segurança do ecossistema é centralizada na Interface de Usuário (UI), que integra uma carteira embarcada e o novo motor criptográfico baseado em senhas mestras. A solução abandona a dependência de bibliotecas legadas e adota um esquema de proteção local onde a chave privada do usuário é cifrada via AES-256-CGM, com chaves derivadas pelo algoritmo PBKDF2 a partir de uma senha de conhecimento exclusivo do titular. Esse mecanismo de *keystore* garante que, embora o sistema facilite o acesso, a soberania sobre as chaves de assinatura e decifragem permaneça estritamente com o usuário final.

Em relação à privacidade, a proposta introduz uma distinção clara no tratamento dos dados. Informações sobre cursos, disciplinas e notas são enviadas em lote e armazenadas de forma pública dentro da blockchain, garantindo integridade e auditabilidade sem revelar a identidade do aluno. A proteção da identidade é realizada no momento do registro do estudante, onde seus dados sensíveis (nome e documento) são cifrados via ECIES utilizando chaves públicas. O controle condicional de acesso é mantido através de um modelo onde o estudante pode recifrar seus dados de identificação para terceiros solicitantes, utilizando suas respectivas chaves privadas recuperadas via senha mestra.

E, visando a sustentabilidade econômica, a arquitetura é projetada para execução em redes *EVM-Compatible* de baixo custo. Esta escolha, somada à redução do volume de dados cifrados e ao uso de transações em lote, viabiliza a solução para instituições de grande porte. O

resultado é uma infraestrutura que equilibra a transparência necessária ao histórico acadêmico com a segurança rigorosa das identidades digitais, oferecendo um sistema prático, escalável e independente de provedores de carteira tradicionais.

Para fins de transparência e reprodutibilidade técnica, a arquitetura proposta foi disponibilizada integralmente em repositórios públicos. O ecossistema está segregado em três frentes operacionais: o repositório dos contratos inteligentes e scripts de implantação¹, o repositório da interface descentralizada (DApp) contendo o motor criptográfico² e o repositório destinado ao serviço de orquestração e processamento em lote baseado em Airflow³. A integração desses componentes viabiliza o fluxo completo de registro acadêmico, desde a ingestão massiva de dados até a gestão soberana da identidade pelo estudante.

4.5 Modelagem do sistema

Uma vez estabelecida a concepção da arquitetura e o modelo de negócio, este tópico detalha a especificação técnica e a implementação de cada componente da solução. A modelagem foca na tradução dos requisitos funcionais em estruturas de dados, algoritmos e fluxos operacionais, detalhando o funcionamento interno do contrato inteligente, a lógica do serviço de orquestração e os mecanismos criptográficos que garantem a soberania do estudante sobre sua identidade digital.

4.5.1 Aplicação de escalabilidade ao contrato inteligente

A implementação do contrato *AcademicRecordStorage* foi projetada para expandir a estrutura lógica do sistema-base, preservando a integridade das entidades fundamentais (*Institution*, *Student*, *Course*, *Discipline* e *Grade*) e os mecanismos de controle de acesso. No entanto, o contrato original operava sob uma arquitetura de escrita individualizada, onde cada inserção exigia uma transação exclusiva. Para uma instituição de ensino, esse modelo representava uma barreira operacional crítica, visto que o registro de uma única turma demandaria centenas de assinaturas manuais via interface de carteira.

Para viabilizar a escalabilidade necessária, foram desenvolvidas funções que permitem a agregação de dados institucionais em uma única chamada (*batch*). Esta abordagem foca na

¹<https://github.com/cefet-records/records-smart-contract>

²<https://github.com/cefet-records/records-dapp>

³<https://github.com/cefet-records/records-batch>

otimização da *Ethereum Virtual Machine* (EVM), reduzindo o custo fixo de transação que seria replicado em chamadas múltiplas. Abaixo, apresentam-se as assinaturas das principais funções implementadas:

Listing 4.1: Assinaturas das funções de processamento em lote

```

1  function addBatchStudents(
2      BatchStudentPayload[] calldata _studentsInfo
3  ) public onlyInstitution;
4
5  function addBatchCourses(
6      address _institutionAddress,
7      BatchCoursePayload[] calldata _coursesInfo
8  ) public institutionExists(_institutionAddress) onlyInstitution
9      ;
10
11 function addGlobalBatchDisciplines(
12     address _institutionAddress,
13     FullDisciplinePayload[] calldata _fullDisciplinesInfo
14 ) public institutionExists(_institutionAddress) onlyInstitution
15     ;
16
17 function addBatchGrades(
18     address _institutionAddress,
19     BatchGradePayload[] calldata _gradesInfo
20 ) public institutionExists(_institutionAddress) onlyInstitution
21     ;

```

A reestruturação permite que as funções *addBatchStudents* e *addBatchCourses* cadastrem, respectivamente, o aluno e a grade de cursos de forma massiva. Além disso, a *addGlobalBatchDisciplines* possibilita o registro de disciplinas realizando validações de unicidade de forma agregada. A gestão do desempenho acadêmico também foi otimizada através da *addBatchGrades*, que processa o envio coletivo de históricos sob verificações rigorosas de consistência entre os códigos de disciplina e o curso do aluno antes da persistência dos dados na blockchain.

Esta modelagem transforma o protótipo anterior em uma infraestrutura preparada para altas cargas de dados. Ao eliminar a necessidade de assinaturas redundantes, o sistema agiliza o fluxo administrativo e torna o armazenamento em blockchain economicamente sustentável pela diluição das taxas de *gas*. Por fim, embora o contrato mantenha as funcionalidades de solicitação de acesso (*requestAccess*) e campos cifrados herdados de Pedrosa et al. [2025], a lógica interna

foi simplificada ao remover dependências de bibliotecas externas para manipulação de chaves. O resultado é um sistema mais resiliente a mudanças nos padrões de provedores de carteiras e tecnicamente superior para operar em cenários institucionais reais.

4.5.2 Serviço de processamento em lote para ingestão de registros

Com o intuito de superar as limitações de escalabilidade e reduzir a carga de interações manuais repetitivas, se propõe a implementação de um serviço de orquestração e processamento em lote (*batch*). A principal função desse serviço é automatizar a ingestão periódica de registros acadêmicos, permitindo que a instituição realize o tratamento de grandes volumes de dados de maneira eficiente e segura antes da persistência final. Essa abordagem estratégica desloca a lógica de preparação de dados para o ambiente externo a blockchain (camada de serviço), otimizando o fluxo operacional e permitindo que a gravação na blockchain ocorra de forma consolidada ao final de períodos letivos ou ciclos administrativos específicos.

O fluxo de funcionamento do serviço é coordenado por um orquestrador baseado em *Apache Airflow*, que gerencia a execução de Directed Acyclic Graphs (DAGs) customizadas para cada entidade do sistema. Cada DAG representa um fluxo de trabalho estruturado em um conjunto de tarefas (*tasks*) sequenciais e interdependentes, garantindo a atomicidade e a rastreabilidade do processo. O ciclo de vida de uma ingestão inicia-se com tarefas de varredura no diretório de registros acadêmicos, onde o serviço busca diversos arquivos em formato CSV contendo tuplas de dados para estudantes, cursos, disciplinas e notas.

Uma vez localizados os arquivos, as tarefas subsequentes realizam o tratamento, a limpeza e a organização estrutural das informações, validando a integridade dos dados brutos. Diferente de modelos totalmente automatizados que interagem diretamente com a rede, esta arquitetura utiliza um banco de dados *PostgreSQL* como camada intermediária de persistência. Após o processamento das DAGs, os dados tratados são armazenados no banco, onde permanecem organizados por entidade e aguardam a validação final da instituição.

O encerramento do fluxo ocorre através do *DApp*, onde o administrador da instituição de ensino visualiza os lotes preparados pelo serviço de orquestração. Ao acionar os gatilhos de armazenamento via interface, o sistema recupera os registros do banco de dados para realizar a cifragem e a montagem dos *payloads* de transação. Essa interação manual controlada garante que a autoridade emissora tenha governança total sobre o momento da publicação na blockchain, permitindo que uma única operação de rede processe centenas de registros de uma

entidade específica. A adoção deste modelo de processamento em lote, suportado por tarefas orquestradas e uma camada de *buffer* em banco de dados, oferece ganhos significativos de desempenho e confiabilidade, resolvendo erros de entrada manual e otimizando os custos de *gas* ao consolidar a escrita de dados acadêmicos na blockchain.

Contudo, a introdução dessa camada de orquestração e persistência fora da blockchain estabelece novos perímetros de atenção quanto à governança e segurança do pipeline. Ao concentrar o processamento inicial em componentes como o *Airflow* e o *PostgreSQL*, a arquitetura assume uma configuração híbrida, onde a eficiência operacional institucional é balanceada pela confiança descentralizada da rede. Para mitigar os riscos inerentes à centralização temporária dos dados, o desenho da solução mantém a obrigatoriedade da assinatura transacional da autoridade institucional no momento da submissão. Dessa forma, o serviço atua como um facilitador de orquestração, enquanto a responsabilidade final e a trilha de auditoria imutável permanecem vinculadas à identidade soberana da instituição na blockchain, garantindo que a integridade dos registros prevaleça independentemente do processamento intermediário realizado.

4.5.3 Solução criptográfica e modelo de controle condicional de registros

A solução criptográfica deste trabalho fundamenta-se em um modelo híbrido de confidencialidade seletiva, no qual apenas as informações de identificação pessoal do estudante são cifradas fora da blockchain antes do seu armazenamento dentro da rede. Esta abordagem visa conciliar a privacidade dos dados sensíveis com a transparência de registros acadêmicos, otimizando o custo de *gas* ao evitar operações criptográficas onerosas dentro da EVM.

O foco desta arquitetura é a gestão autônoma de identidades. Como ilustrado na Figura 5, o processo inicia-se no *DApp* com a geração de entropia para a criação de um par de chaves assimétricas baseadas em Criptografia de Curvas Elípticas (ECC) sobre a curva *secp256k1*. Simultaneamente, a senha mestra de conhecimento exclusivo da instituição é fornecida e utilizada no algoritmo PBKDF2 para derivar uma chave simétrica, que, em conjunto com um *Salt* e um Vetor de Inicialização (IV), cifra a chave privada gerada através do padrão AES-256-CGM. Para a persistência na blockchain, o *DApp* interage com o contrato inteligente enviando a chave pública da instituição, enquanto a chave privada cifrada é exportada em um arquivo de *backup* JSON para o usuário.

É importante ressaltar que o modelo de backup JSON e senha mestra transfere integralmente a responsabilidade de custódia ao usuário. A perda de ambos os componentes resulta na ina-

cessibilidade irreversível dos dados cifrados. Para mitigar esse risco em cenários produtivos, estratégias de recuperação social (*Social Recovery*) ou o uso de guardiões delegados poderiam ser integrados, permitindo a rotação de chaves sem comprometer a autonomia do titular

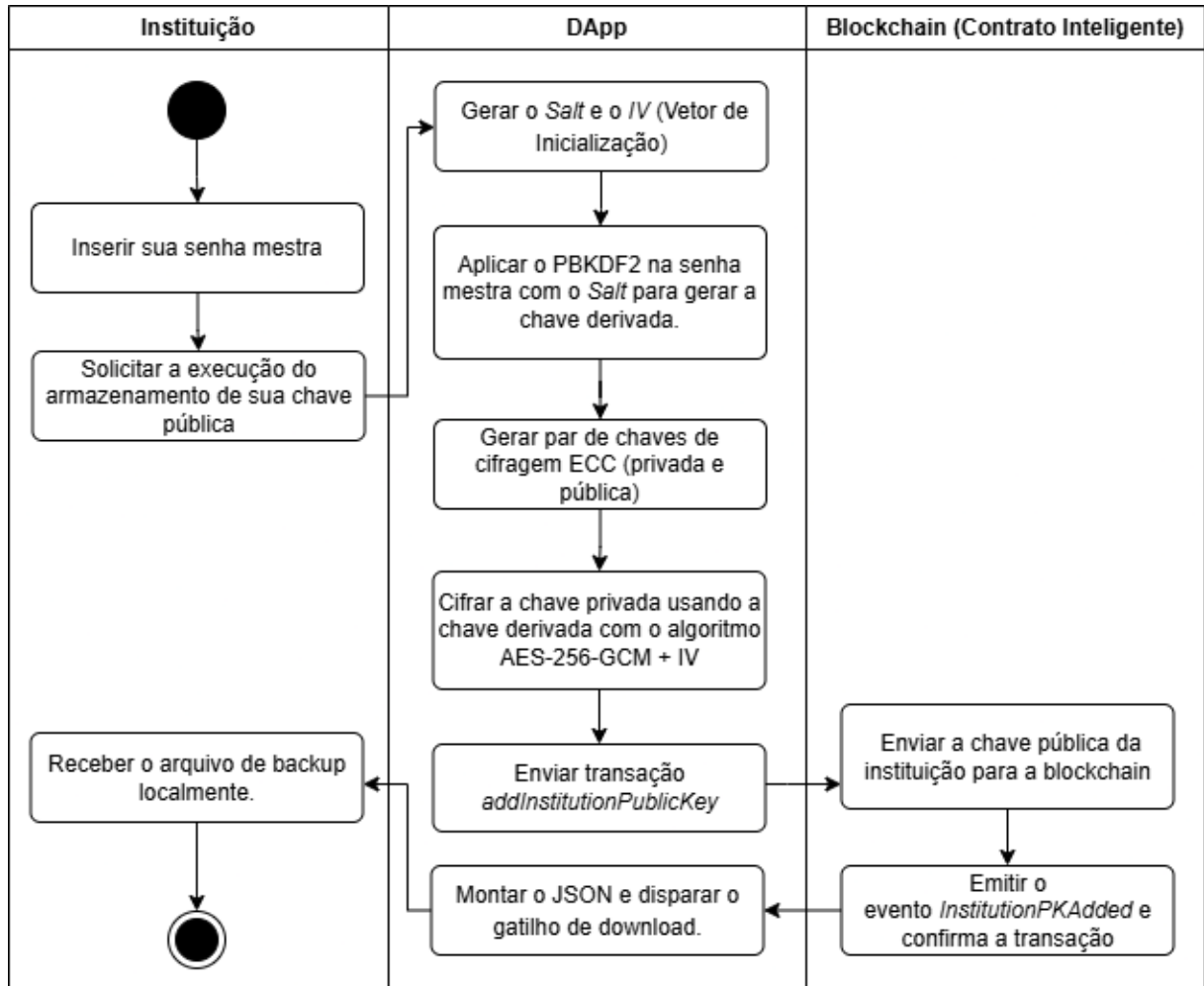


Figura 5: Fluxo criptográfico da instituição e geração de chave pública

No registro do estudante, ilustrado na Figura 6, a proteção da identidade utiliza o esquema Elliptic Curve Integrated Encryption Scheme (ECIES). O *DApp* atua como orquestrador, gerando o par de chaves ECC do estudante e recuperando a chave pública da instituição diretamente da blockchain. Esses dados sensíveis do estudante (nome e documento) são cifrados duplamente: uma vez com a chave pública do estudante e outra com a da instituição. Após a proteção dos dados, a chave privada do aluno é blindada pelo mesmo processo de AES/PBKDF2 descrito anteriormente. O fluxo encerra-se com o envio da transação `addStudentInformation` para a blockchain, que valida o remetente e persiste os registros, enquanto o usuário recebe seu backup local.

O controle condicional de acesso é viabilizado pela cooperação entre visitante e estudante.

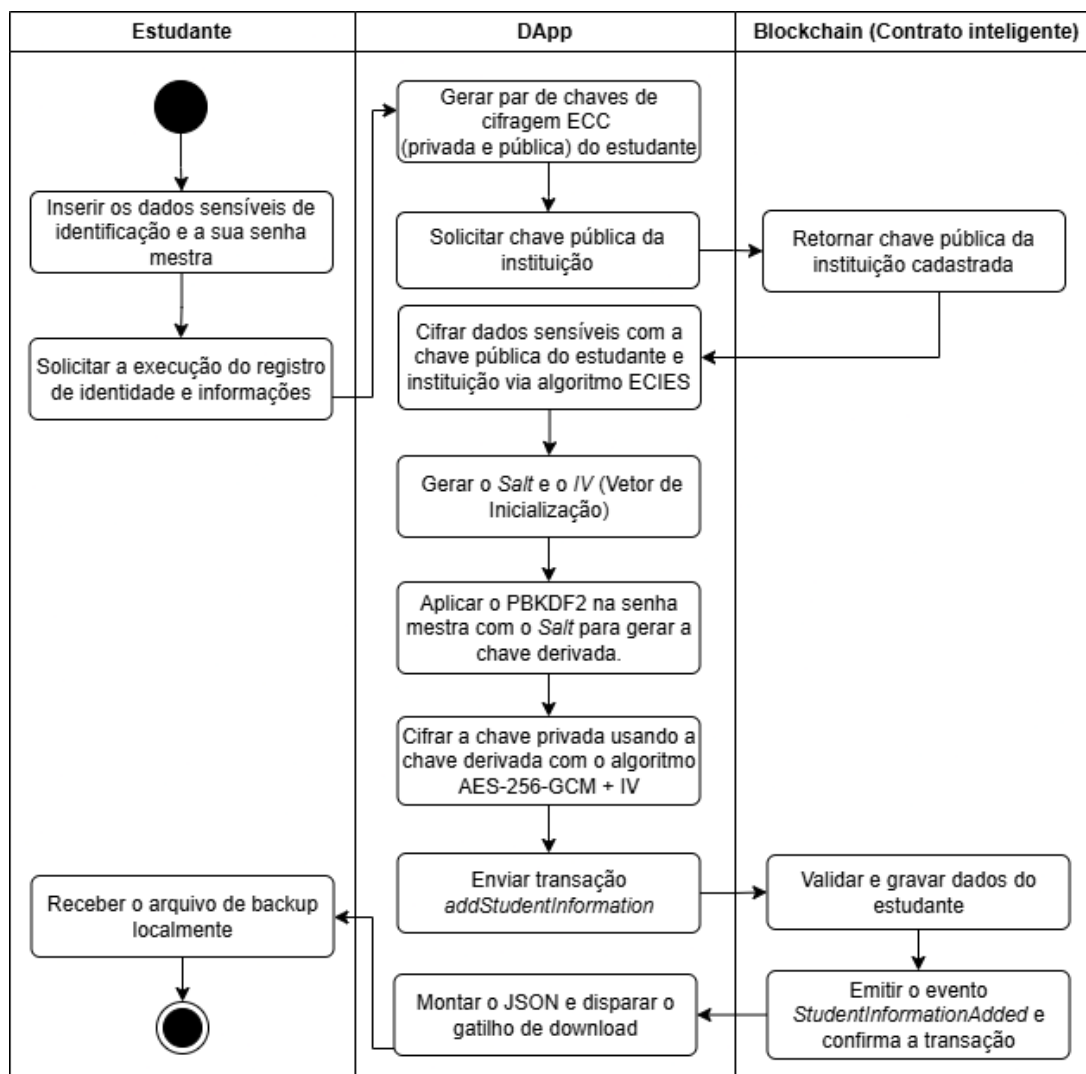


Figura 6: Fluxo criptográfico de registro do estudante

Na Figura 7, observa-se que o visitante, ao solicitar acesso, gera sua própria identidade criptográfica e registra sua chave pública no contrato inteligente através da função `requestAccess`. Este registro é fundamental para que o estudante possa, posteriormente, realizar a recifragem direcionada.

A concessão efetiva do acesso, ilustrado na Figura 8, exige que o estudante recupere sua chave privada a partir do seu backup JSON e sua senha mestra. O *DApp* busca na blockchain a chave pública do visitante solicitante e os dados cifrados do estudante. Após decifrar seus próprios dados, o estudante os cifra novamente utilizando a chave pública do visitante via ECIES. Esta nova versão dos dados é enviada à rede via transação `addEncryptedInfoWithRecipientKey`, garantindo que apenas o visitante específico possa ler a identidade do aluno.

Embora este modelo de recifragem direcionada mantenha um gargalo operacional ao exigir a ação deliberada do estudante para cada concessão, essa escolha de projeto prioriza a soberania

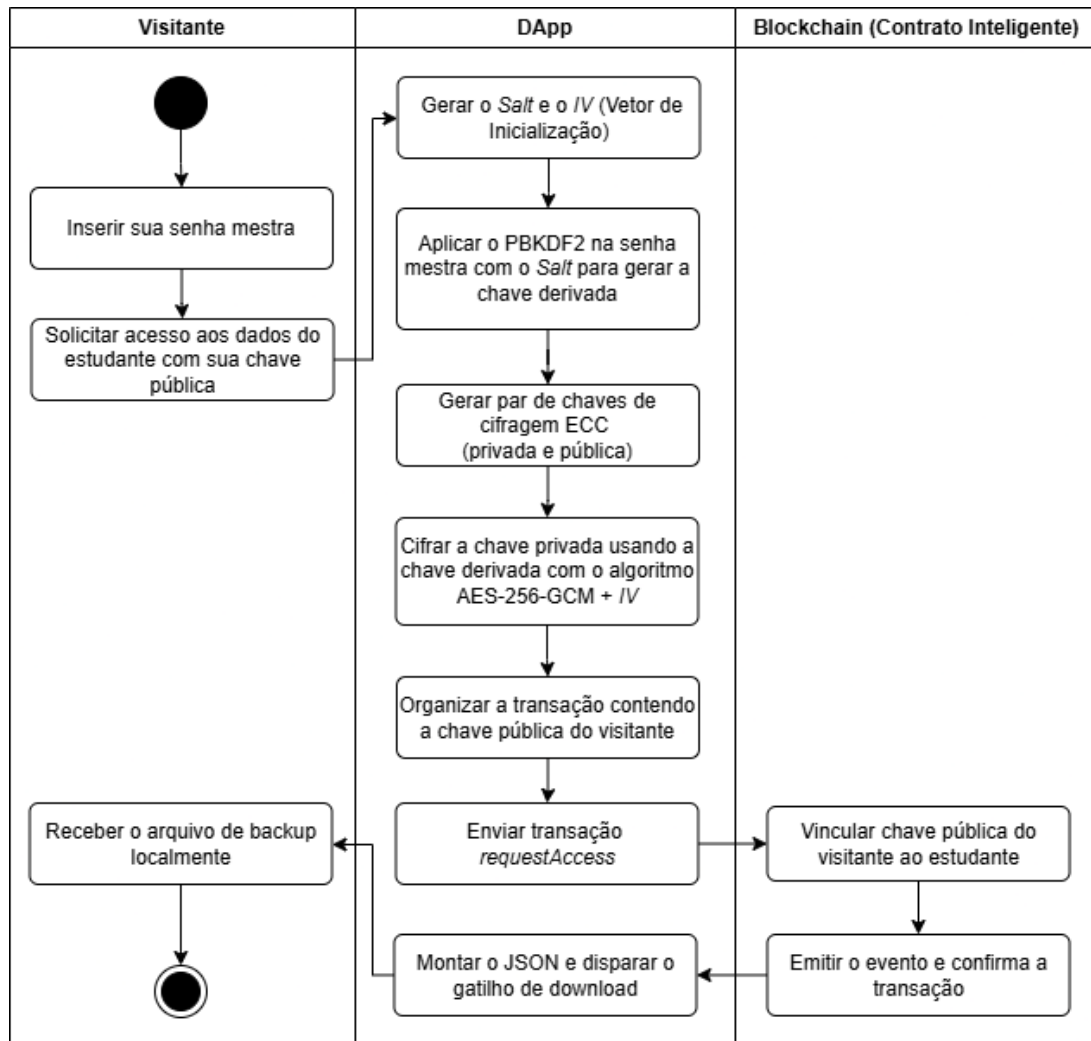


Figura 7: Fluxo de solicitação de acesso pelo visitante

absoluta do proprietário sobre seus dados. Diferente de sistemas de *Proxy Re-Encryption* automatizados, onde servidores terceiros realizam a transposição de chaves, a arquitetura proposta garante que nenhum dado sensível possa ser compartilhado sem o consentimento transacional e a intervenção direta do estudante, eliminando riscos de vazamento por intermediários.

Por fim, o processo de decifragem, comum a todos os usuários autorizados, é detalhado na Figura 9. O usuário fornece seu backup e sua senha mestra, permitindo que o *DApp* reconstrua a chave privada ECC. O payload cifrado é recuperado da blockchain e decifrado via ECIES. O resultado é convertido para um formato legível e apresentado em tela. Este modelo elimina a dependência de bibliotecas legadas e proprietárias, como a *@metamask/eth-sig-util*, utilizando uma implementação agnóstica que garante a longevidade e a segurança da solução em um ambiente descentralizado e autônomo.

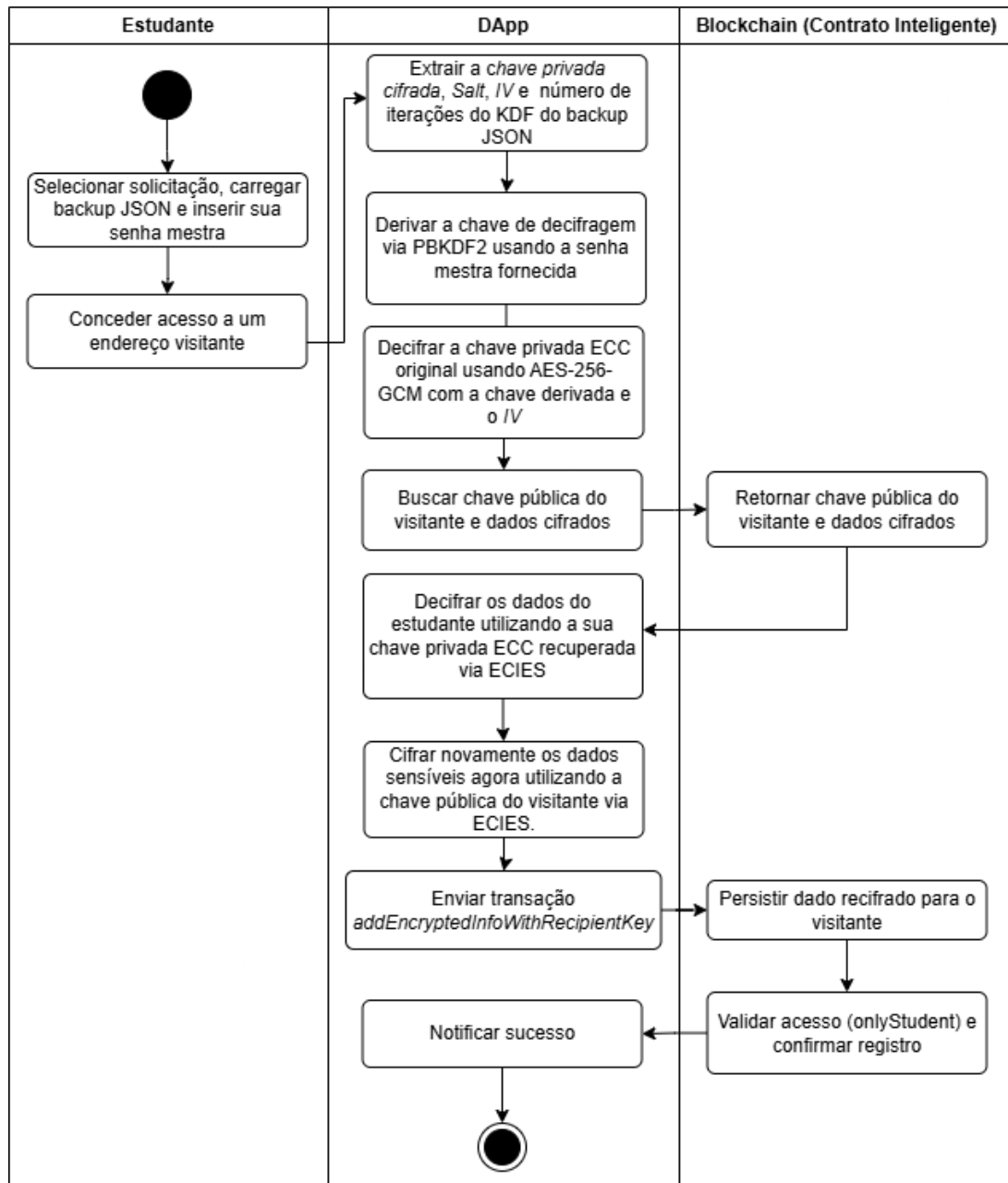


Figura 8: Fluxo de recifragem e concessão de acesso

4.5.4 Abstração de complexidade via carteiras embarcadas e protocolos de autenticação social

Uma das limitações críticas observadas no sistema base proposto por Pedrosa et al. [2025] reside na barreira de entrada imposta pela experiência de *onboarding*. A dependência de interfaces de carteiras externas em formato de extensão, como a *MetaMask*, aliada à custódia manual de frases de recuperação (*seed phrases*), impõe uma carga cognitiva que afasta perfis não técnicos. Para resolver esse problema, este trabalho integra o conceito de carteiras embar-

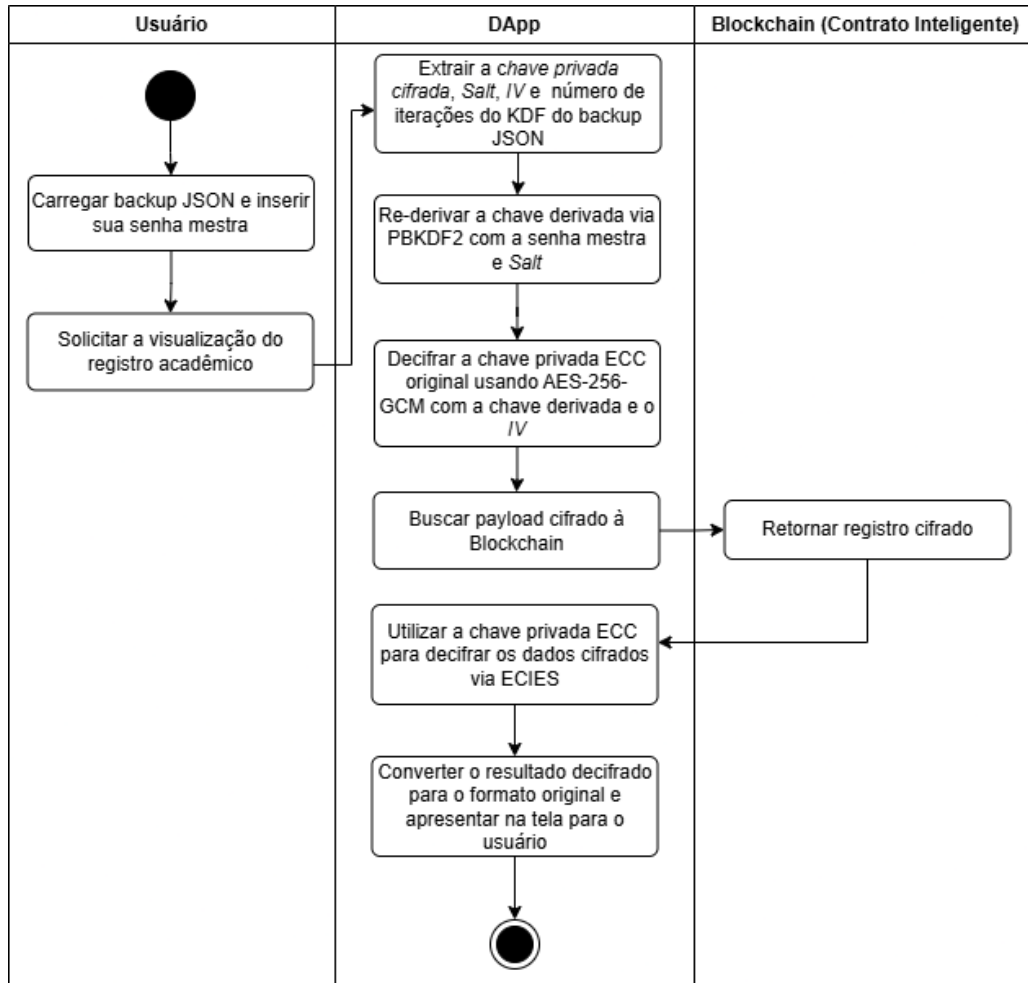


Figura 9: Fluxo universal de decifragem de dados

çadas (*embedded wallets*), uma arquitetura que abstrai a complexidade da *Web3* ao transformar a gestão de chaves em um processo transparente.

Tecnicamente, essa simplificação é viabilizada por plataformas de orquestração de identidade como a *Dynamic*. O diferencial técnico reside na utilização de protocolos de autenticação tradicionais, como *OAuth2* e *OpenID Connect* (OIDC), para realizar a geração de identidades criptográficas. Ao realizar o *login* via redes sociais (*Google, Apple, etc.*), o sistema utiliza o *token* de identidade (ID Token) assinado pelo provedor para autorizar a criação de uma carteira vinculada de forma única ao identificador do usuário na plataforma legada [Labs, 2024].

A segurança dessa operação é garantida por tecnologias de Computação Multipartidária (MPC - *Multi-Party Computation*), que fragmentam a chave privada em múltiplas partes (*shares*). Diferente do modelo convencional onde a chave reside integralmente no dispositivo do usuário ou no servidor, o modelo MPC garante que a chave privada nunca seja reconstruída em um único local, exigindo a cooperação entre o dispositivo do usuário (autenticado via *passkeys*

ou métodos biométricos) e o provedor de infraestrutura para assinar transações.

Dessa forma, a plataforma elimina a necessidade de configurações manuais de rede (RPC) e a gestão de ativos para pagamento de taxas (*gas*), permitindo que estudantes e instituições interajam com o contrato inteligente através de uma interface familiar. Ao associar automaticamente o e-mail do usuário a um endereço blockchain, o sistema provê a persistência necessária para o gerenciamento de chaves simétricas e identidades digitais, sem comprometer a segurança da custódia dos dados acadêmicos.

Apesar das vantagens significativas em termos de usabilidade e redução da barreira de entrada, a adoção de carteiras embarcadas baseadas em provedores externos, como a Dynamic, introduz novas assunções de confiança que devem ser explicitadas. Diferentemente do modelo clássico de autocustódia plena, no qual o usuário detém controle exclusivo sobre sua chave privada, o modelo de carteiras embarcadas com MPC estabelece uma custódia distribuída e dependente de infraestrutura de terceiros.

Nesse contexto, a disponibilidade operacional do sistema passa a depender do provedor de carteira embarcada, uma vez que a assinatura de transações exige a cooperação entre o dispositivo do usuário e os serviços do provedor. Eventuais falhas, interrupções de serviço ou descontinuidade da plataforma podem impactar temporariamente a capacidade dos usuários de interagir com a blockchain, ainda que os dados acadêmicos permaneçam imutáveis e verificáveis na blockchain.

Além disso, há uma assunção de confiança relacionada à governança e à segurança do provedor, uma vez que ataques à infraestrutura, falhas de implementação ou mudanças unilaterais de política podem afetar o modelo de custódia adotado. Embora a utilização de MPC reduza significativamente o risco de comprometimento direto da chave privada, ela não elimina completamente a dependência institucional do serviço.

Portanto, a autonomia proporcionada ao aluno neste trabalho deve ser compreendida como uma autonomia funcional e de uso, caracterizada pela eliminação de complexidades técnicas, como gestão manual de *seed phrases* e configuração de redes, e não como uma autonomia criptográfica absoluta. Tal escolha é deliberada e alinhada ao objetivo do sistema, que prioriza acessibilidade, inclusão digital e adoção em larga escala no contexto educacional, reconhecendo os *trade-offs* inerentes à solução adotada.

4.5.5 Infraestrutura em rede EVM-Compatible para viabilidade econômica

Com o objetivo de viabilizar o uso prático da solução em um ambiente acadêmico real, este trabalho adota a rede *Polygon* (anteriormente *Matic*) como infraestrutura de Camada 2 (*Layer 2*) compatível com a *Ethereum Virtual Machine* (EVM). Essa escolha é estratégica para garantir que a arquitetura proposta mantenha a segurança e a descentralização do ecossistema *Ethereum*, mas supere as barreiras financeiras impostas pelas taxas de transação (*gas fees*) elevadas da rede principal.

A utilização de uma rede *EVM-Compatible* permite que o desenvolvimento de contratos inteligentes seja realizado em *Solidity*, aproveitando a maturidade das ferramentas de desenvolvimento, como *Hardhat* e *Wagmi*, e garantindo que a lógica de negócio seja portátil entre diferentes redes compatíveis. Tecnicamente, a *Polygon* opera através de um mecanismo de consenso de prova de participação (*Proof of Stake - PoS*) em uma *sidechain* vinculada à *Ethereum*, o que permite processar um volume de transações significativamente maior com tempos de confirmação de blocos reduzidos.

Essa escolha de infraestrutura é fundamental para suportar o modelo de orquestração externa ao blockchain em lote desenvolvido nesta pesquisa. Ao integrar uma rede de baixo custo à arquitetura, o sistema torna-se capaz de absorver fluxos de dados intensos, comuns em processos de encerramento de períodos letivos, sem que o custo transacional inviabilize a operação da instituição de ensino. Assim, a rede *Polygon* atua como a camada de persistência eficiente, equilibrando a necessidade de imutabilidade dos registros acadêmicos com os requisitos de escalabilidade e sustentabilidade financeira do projeto.

Capítulo 5

Avaliação experimental e resultados

Neste capítulo, apresentam-se a metodologia utilizada, bem como a demonstração do fluxo operacional e os resultados obtidos através da execução dos experimentos planejados, visando validar a eficiência, segurança e viabilidade econômica da solução proposta em comparação ao sistema-base.

5.1 Metodologia e ambiente de testes

Para a validação da solução proposta e a comprovação das melhorias de desempenho em relação ao sistema-base, estabeleceu-se um protocolo experimental focado na simulação de cenários operacionais reais de uma instituição de ensino. A metodologia adotada buscou quantificar o ganho de eficiência na ingestão de dados e na preparação criptográfica, permitindo uma comparação entre o esforço de transações individuais do modelo original e a arquitetura de orquestração em lote.

O ambiente de execução dos testes foi padronizado em uma estação de trabalho equipada com processador AMD Ryzen 7 5700G, 32 GB de memória RAM DDR4, operando sob o sistema operacional Windows 11. A infraestrutura de microsserviços foi composta pelo orquestrador de fluxos *Apache Airflow* v2.10.5, executando tarefas em *Python* para o processamento dos arquivos CSV, e um banco de dados relacional *PostgreSQL* 17.2 atuando como camada de *buffer*. Para a interface do usuário e integração com a rede, utilizou-se o ambiente *Node.js* v22.14.0, integrando o *framework* *Next.js* e as bibliotecas *Wagmi* e *Viem* para a comunicação com o contrato inteligente.

A camada de consenso foi simulada localmente utilizando a ferramenta *Hardhat Network*, instanciando um nó de *blockchain* compatível com EVM. Esta abordagem garantiu a precisão das métricas de consumo de *gas* e latência de processamento local, isolando os testes de instabilidades ou congestionamentos de redes públicas externas.

O protocolo experimental foi estruturado em quatro cenários de complexidade progressiva, definidos pela volumetria das entidades acadêmicas (*students*, *courses*, *disciplines* e *grades*).

O fluxo consistiu na ativação das DAGs no *Airflow* para a ingestão dos registros a partir de arquivos CSV, seguida pela validação e armazenamento no *PostgreSQL*. Posteriormente, através do *DApp*, disparou-se o armazenamento em lote na *blockchain*, onde foram medidos os tempos de execução do serviço de *batch* e a latência de cifragem asssimétrica no cliente. A eficácia da solução foi validada pelo sucesso do ciclo completo: desde a derivação da chave via senha mestra e cifragem ECIES local, até a confirmação da transação na blockchain e a posterior recuperação e decifragem do dado pelo destinatário. Para melhor compreensão da integração entre esses componentes técnicos e a experiência do usuário final, a seção a seguir apresenta a demonstração visual e o fluxo operacional do sistema.

5.2 Demonstração do funcionamento e fluxo operacional do DApp

O funcionamento da aplicação desenvolvida materializa a arquitetura proposta através de uma jornada de usuário dividida em quatro fases críticas: autenticação, gestão institucional, ingestão de dados e controle soberano de acesso. O ciclo de vida do sistema inicia-se na interface de login, que utiliza o protocolo da *Dynamic* para oferecer uma experiência de Web2-to-Web3. Diferente de soluções tradicionais que impõem a curva de aprendizado de extensões como a *MetaMask*, o sistema permite que o usuário gere sua carteira embarcada através de provedores de identidade social, como o Google, conforme ilustrado na Figura 10.

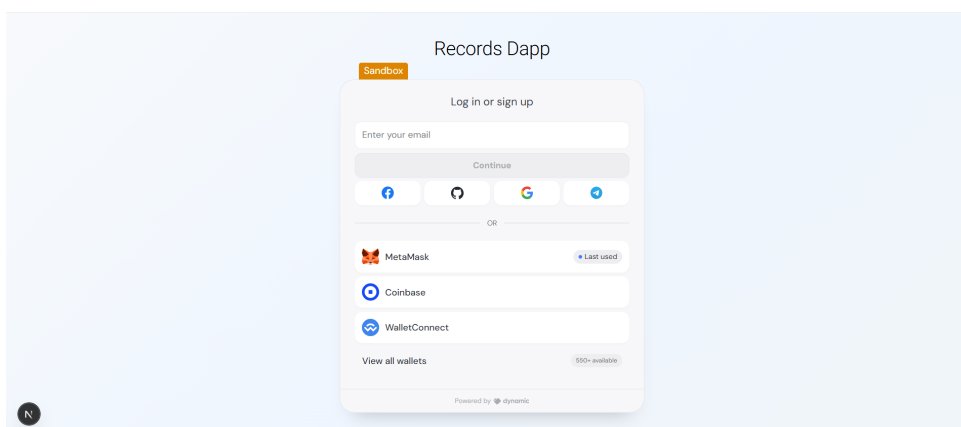


Figura 10: Interface de autenticação com suporte a login social e geração de carteira embarcada.

Uma vez estabelecida a identidade digital, o fluxo operacional segue para o domínio administrativo, onde o dono do contrato assume o papel de autorizador, registrando os endereços públicos das instituições de ensino parceiras (Figura 11). Este processo pressupõe uma etapa de validação externa, onde o endereço público da instituição é fornecido à administração por

canais seguros de comunicação institucional. Após a autorização, a instituição de ensino realiza seu próprio registro de informações institucionais, conforme ilustrado na Figura 12, e passa a gerenciar a ingestão de dados em lote (Figura 13). O primeiro passo da instituição é o cadastro dos endereços públicos de seus estudantes, também obtidos de forma externa, seja via sistemas acadêmicos pré-existentes ou e-mail. Com os estudantes habilitados, o sistema permite que estes realizem o preenchimento de suas informações pessoais sensíveis, como nome e CPF (Figura 14), que são cifradas localmente via ECIES antes de serem enviadas para a camada de consenso.

Records dApp

Hardhat 0x43.2266

Registrar endereço da instituição

Como Owner, você pode registrar o endereço de uma nova instituição. A instituição precisará atualizar seu perfil e gerar suas próprias chaves em um componente separado.

Endereço da Instituição (0x...)*
0x9f69A815356baFce6a4f819d1b92bC26bFa053Ae

Hash da Transação: 0x2241d998b5148719e69e13136e77f90febbe3e7212b1a4fc7ca5c7024ce9e653

REGISTRAR

Figura 11: Processo de autorização institucional realizado pelo administrador do contrato.

Records dApp

Hardhat 0x43.2266

Registrar informações da sua instituição

Nome da Instituição * CEFET/RJ

CNPJ / Documento * 00.000.000/0000-00

Senha Mestra de Criptografia *

Esta senha cifra sua chave privada. NÃO A PERCA.

Requisitos da Senha:

- ✓ Mínimo 12 caracteres
- ✓ Letras maiúsculas e minúsculas
- ✓ Números e caracteres especiais

REGISTRAR E GERAR CHAVES

Estudantes Cursos Disciplinas Notas

Figura 12: Processo de cadastro das informações da instituição de ensino.

A fase de maior densidade operacional ocorre com a execução dos lotes de registros acadêmicos. A instituição, através de sua interface, dispara sequencialmente as transações de Cursos, Disciplinas e Notas (Figura 15), consolidando o histórico acadêmico na blockchain. A partir deste ponto, o dado torna-se imutável e acessível para consulta pelo detentor da nota, que utiliza sua senha mestra para descriptografar e visualizar o histórico em tempo real (Figura 16).

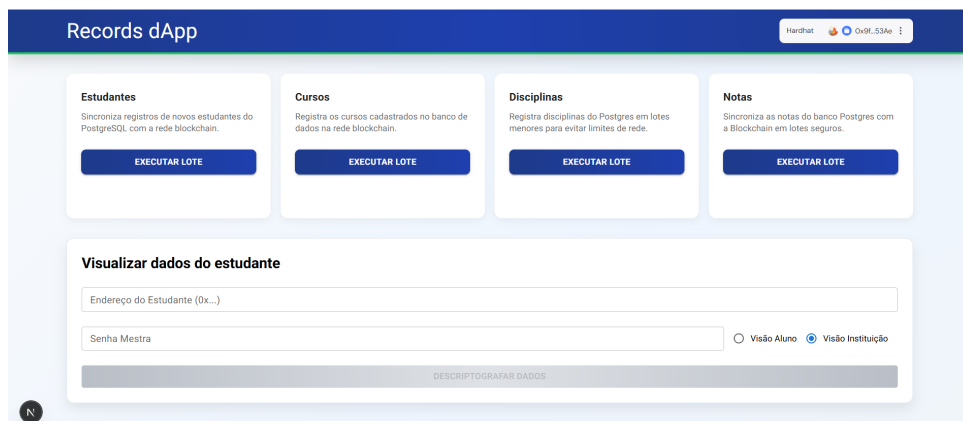


Figura 13: Tela da instituição com botões para ingestão em lote



Figura 14: Interface de preenchimento e cifragem de dados pessoais pelo estudante.

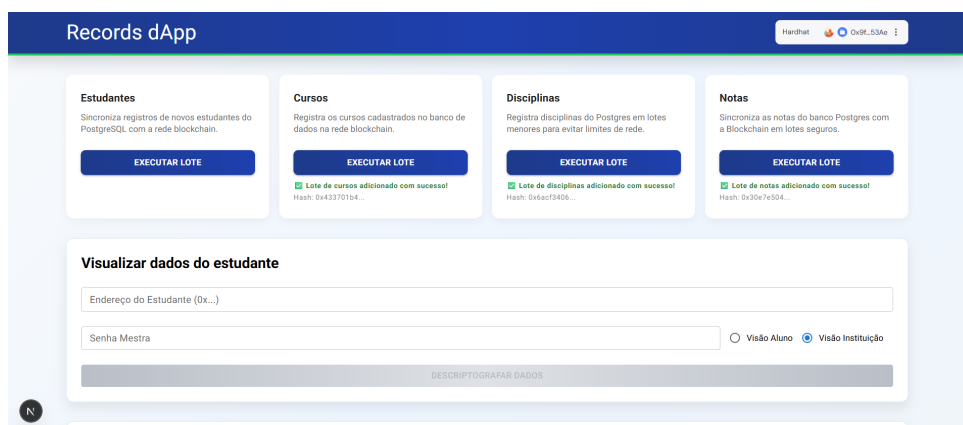


Figura 15: Confirmação de execução das operações de batching na blockchain.

A privacidade final é garantida pelo modelo de controle condicional de acesso. Quando um visitante externo deseja verificar os registros, ele deve primeiramente fornecer seu endereço público ao aluno. Na aplicação, o visitante solicita formalmente o acesso ao perfil do estudante (Figura 17). O aluno, ao identificar a solicitação pendente, executa o processo de recifragem: sua chave privada recuperada via senha mestra decifra o dado original e o recifra utilizando a

Consulta de histórico acadêmico

Endereço do Estudante (Dx...)
0x0775f8e1bE4A82B3531ec4B81897E87442F8Ae3

Senha Mestra

VISUALIZAR HISTÓRICO

Detalhes do Histórico

Nome do Estudante: Juan Camacho Silva de Lima
Endereço do Estudante: 0x0775f8e1bE4A82B3531ec4B81897E87442F8Ae3

Curso: SEC - Ciência da Computação
Documento do Estudante: 000.000.000.000
Hash do Documento (Blockchain): Dec9fC7a9bdc1a02b25b778a4c22a4a294429f23a059Caa7C2a2

CODIGO	DISCIPLINA	CARGA HORÁRIA	PROFESSOR	NOTA	FREQUÊNCIA	STATUS
HISTÓRICO 1						
ALC301	Álgebra Linear Computacional	75	5	95.00	90%	Aprovado
CAL101	Cálculo Diferencial e Integral I	90	6	85.00	95%	Aprovado
HISTÓRICO 2						
EST201	Estruturas de Dados	75	5	78.00	88%	Aprovado
MAT102	Cálculo Diferencial e Integral II	90	6	70.00	82%	Aprovado
HISTÓRICO 3						
SEC401	Segurança da Informação	90	6	45.00	100%	Reprovado
SOC302	Sistemas Operacionais	60	4	92.00	100%	Aprovado
TC302	Teoria da Computação	60	4	65.00	75%	Aprovado
HISTÓRICO 4						
CMP401	Computações	75	5	72.00	90%	Aprovado
LLA07	Inteligência Artificial	60	4	88.00	90%	Aprovado

Figura 16: Painel de visualização do histórico acadêmico decifrado localmente pelo aluno.

chave pública do visitante (Figura 18), portanto neste momento, o visitante também conseguirá visualizar os registros acadêmicos do estudante bem como está na Figura 16. Este fluxo assegura que apenas as partes autorizadas possuam as chaves de decifragem, eliminando a possibilidade de vazamento de dados por terceiros ou pela própria instituição emissora, completando assim o modelo de segurança e transparência proposto.

Records dApp

Ver chat 0x077...A2Bf

Solicitar acesso à informação do estudante
 Gere um novo par de chaves, salve o backup da sua chave privada e, em seguida, solicite acesso aos registros de um estudante enviando sua chave pública. O estudante precisará aprovar sua solicitação.

Endereço do Estudante (Dx...)
0x0775f8e1bE4A82B3531ec4B81897E87442F8Ae3

Senha Mestra

GERAR PAR DE CHAVES E BACKUP

SOLICITAR ACESSO AO ESTUDANTE

Consulta de histórico acadêmico

Endereço do Estudante (Dx...)

Senha Mestra

Figura 17: Interface do visitante para requisição de acesso a registros de terceiros.

5.3 Desempenho do serviço de orquestração em lote

A avaliação do desempenho do serviço de orquestração é fundamental para validar a viabilidade operacional do modelo proposto, especialmente no que tange ao processamento de grandes volumes de dados acadêmicos. O fluxo operacional inicia-se com a coleta de arquivos estruturados em formato CSV, contendo informações de estudantes, cursos, disciplinas e notas, que são submetidos ao serviço de *batch*. Este componente utiliza o *Apache Airflow* para gerenciar DAGs que executam a triagem, o tratamento e a normalização dos dados antes de sua

Figura 18: Processo do aluno conceder acesso aos registros acadêmicos para o visitante.

persistência no banco de dados *PostgreSQL*. Esta etapa intermediária é estratégica, pois permite que a instituição revise a integridade das informações e corrija eventuais erros de duplicidade antes do comprometimento definitivo na blockchain.

Para validar a eficiência da arquitetura, foram estabelecidos quatro cenários experimentais de complexidade crescente. O cenário 1 serviu como linha de base (2 estudantes, 2 cursos, 4 disciplinas e 3 notas), enquanto o cenário 2 expandiu a carga para volumes moderados (30 notas e 15 disciplinas). Os cenários 3 e 4 foram projetados para estresse de sistema, simulando o fechamento de períodos letivos com 100 e 500 registros de notas, respectivamente. Os tempos registrados contemplam tanto a latência da ingestão automatizada pelo orquestrador quanto o tempo de resposta do *DApp* durante as operações de cifragem assimétrica e preparação para o envio à rede.

Cabe apontar que a manutenção do número fixo de dois estudantes em todos os cenários experimentais decorre de uma restrição técnica das cotas de uso do serviço de carteiras embarcadas da *Dynamics*. Por tratar-se de uma operação em camada gratuita, a escalabilidade de usuários foi limitada para garantir a viabilidade dos testes sem extrapolar os limites de instâncias de identidades digitais permitidas pelo provedor. Essa limitação não compromete a validade dos testes de desempenho, visto que o estresse do sistema foi direcionado ao volume de registros acadêmicos (notas e disciplinas), que representam o maior gargalo operacional em cenários reais de fechamento de períodos letivos.

Enquanto no trabalho base a inserção de dados era realizada de forma individual e manual, a implementação em lote demonstrou uma redução drástica no esforço operacional. Como observado na Tabela 3, embora o tempo de processamento no *DApp* apresente um crescimento mais acentuado em lotes maiores (atingindo 58,5 segundos para 500 notas) devido à carga com-

Tabela 3: Resultados consolidados dos testes de desempenho (em segundos)

Cenário	Entidade	Qtd. Registros	Tempo Batch (s)	Tempo DApp (s)
Cenário 1	Estudantes	2	8,24	3,09
	Cursos	2	3,21	0,51
	Disciplinas	4	3,40	0,63
	Notas	3	3,77	3,12
Cenário 2	Estudantes	2	8,00	0,65
	Cursos	5	3,46	0,54
	Disciplinas	15	4,01	0,52
	Notas	30	8,17	4,85
Cenário 3	Estudantes	2	8,15	0,70
	Cursos	5	3,50	0,58
	Disciplinas	30	5,20	1,15
	Notas	100	14,30	12,40
Cenário 4	Estudantes	2	8,30	0,75
	Cursos	10	4,10	0,85
	Disciplinas	100	12,60	3,90
	Notas	500	42,10	58,50

putacional da cifragem ECIES executada no navegador, o serviço de *batch* manteve uma curva de crescimento estável. A latência inicial do *Airflow* (média de 8 segundos para estudantes) reflete o custo fixo de inicialização das DAGs e conexão com o banco de dados, mas o sistema demonstra alta escalabilidade ao processar 500 registros de notas em apenas 42,1 segundos no ambiente.

A eficiência do serviço é confirmada pela capacidade de transformar um processo que levaria horas de preenchimento manual em uma tarefa concluída em cerca de um minuto. Ao utilizar o banco de dados como *buffer*, a solução garante a integridade referencial, prevenindo erros como registros duplicados para o mesmo período, e assegura que a instituição mantenha governança total sobre o envio de dados, validando o modelo de orquestração como uma camada de abstração ágil, segura e plenamente escalável para o ambiente acadêmico.

5.4 Análise de segurança e qualidade do contrato inteligente

A avaliação da confiabilidade e da qualidade do código do contrato inteligente *AcademicRecordStorage* foi realizada por meio da ferramenta de auditoria automatizada *SolidityScan* (Cred Shields). O contrato, composto por 674 linhas de código, obteve uma pontuação de segurança de 61,39/100, sendo classificado com um nível de risco moderado (*Medium Risk*). Esta

análise técnica é fundamental para identificar se as otimizações de escalabilidade introduzidas geraram superfícies de ataque imprevistas na integridade dos registros acadêmicos. Os resultados detalhados indicam que o contrato apresenta uma estrutura sólida em termos de arquitetura de governança, com a ausência de funções maliciosas de cunhagem (*minting*) ou mecanismos de interrupção arbitrária (*pausable*), o que reforça a natureza imutável e a disponibilidade dos registros.

Entretanto, a ferramenta identificou uma vulnerabilidade de severidade crítica e dez de severidade média, majoritariamente associadas à complexidade das funções de processamento em lote e à arquitetura de permissões do sistema. O achado crítico de "risco de acesso especial" refere-se à concentração de privilégios nos modificadores `onlyOwner` e `onlyInstitution`. Embora esse comportamento seja um requisito de negócio para permitir que as instituições gerenciem registros de forma autônoma, reconhece-se que ele estabelece um ponto de falha centralizado que exige justificativa técnica e mecanismos de controle. Para mitigar o risco de abuso, a segurança da solução não repousa apenas na restrição de acesso, mas em um modelo de transparência e auditabilidade por eventos. Todas as funções administrativas críticas emitem eventos indexados, como `InstitutionAdded`, `InstitutionInformationAdded` e `GradeAdded`, permitindo o monitoramento externo e a rastreabilidade total de ações fora da blockchain. Além disso, o endereço do proprietário do contrato é definido como `immutable`, o que impede a transferência maliciosa de controle após a implantação, e o mapeamento `isInstitution` exige uma transação explícita do proprietário para concessão de acesso, criando uma trilha de responsabilidade clara.

Quanto à robustez lógica, a análise automatizada sugere que o controle de acesso implementado é eficaz contra classes comuns de ataques de injeção e manipulação de estado através do uso de modificadores de existência, como `studentExists`, `courseExists` e `disciplineExists`, que garantem a integridade referencial dos dados durante inserções massivas. No entanto, é importante ressaltar que a afirmação de resiliência total do contrato exigiria a aplicação adicional de testes de *fuzzing* ou auditorias formais de invariantes. O uso da versão recente do compilador *Solidity* 0.8.28 também auxilia na proteção nativa contra erros de aritmética, como o estouro de inteiros (*overflow*), mitigando riscos presentes em versões legadas. A densidade de notificações informativas e de otimização de *gas* reflete a complexidade necessária para suportar a lógica de *batching*. Em geral, o contrato inteligente apresenta um avanço em relação à prova de conceito original, equilibrando a introdução de funcionalidades complexas com um *framework* instituci-

onal escalável, onde o perfil de risco moderado é gerenciado pela governança exercida através da transparência dos registros na blockchain.

5.5 Análise comparativa de custos e escalabilidade

A viabilidade de uma solução baseada em blockchain é intrinsecamente ligada à sua eficiência econômica e capacidade de absorver o crescimento da base de dados sem custos proibitivos. Nesta análise, utilizou-se o consumo de *gas* real aferido no cenário 1 como unidade base para a mensuração. Para fins de comparabilidade entre as redes e cenários, fixou-se as cotações do ETH e do POL e o preço médio do *gas* conforme os valores vigentes no momento da coleta, isolando assim a volatilidade do mercado para focar estritamente na eficiência da arquitetura de dados.

No modelo de registros unitários do trabalho base, cada inserção manual gerava uma transação individual, resultando em um acúmulo de taxas de *gas* que tornava a gestão institucional inviável. Com a implementação do serviço de orquestração em lote, a taxa base da transação é diluída entre todos os registros. Conforme demonstrado na Tabela 4, o custo total para o fluxo completo do cenário 1 na rede *Ethereum* totalizou R\$ 81,43, enquanto na rede *Polygon* o valor foi reduzido para aproximadamente R\$ 0,03, uma economia superior a 99,9%.

Tabela 4: Comparativo de custos transacionais detalhado: *Ethereum* vs. *Polygon* (cenário 1)

Operação	Gasto ETH	Custo ETH (R\$)	Gasto POL	Custo POL (R\$)
addInstitution	0,00021600	3,55	0,002160	0,0012
addInstitutionInformation	0,00011808	1,94	0,001181	0,0007
addInstitutionPublicKey	0,00023956	3,94	0,002396	0,0014
addBatchStudents (2 est.)	0,00020354	3,35	0,002035	0,0012
addStudentInformation 1	0,00097400	16,02	0,009740	0,0057
addStudentInformation 2	0,00094083	15,47	0,009408	0,0055
addBatchCourses (2 cursos)	0,00037031	6,09	0,003703	0,0021
addGlobalBatchDisciplines (4 disc.)	0,00104841	17,24	0,010484	0,0061
addBatchGrades (3 notas)	0,00035315	5,81	0,003532	0,0020
requestAccess	0,00019241	3,16	0,001924	0,0011
addEncryptedInfoWithRecipientKey	0,00029580	4,86	0,002958	0,0017
TOTAL	0,00495209	81,43	0,049521	0,0292

A escalabilidade econômica da solução torna-se evidente ao estimarmos os custos para os cenários de estresse na rede *Polygon* (Tabela 5). Estas estimativas baseiam-se no custo de execução das funções de *batch* somado ao custo incremental de armazenamento (*SSTORE*). Um diferencial técnico implementado na interface de usuário é a fragmentação de grandes volumes em sub-lotes (*chunks*). Para garantir a estabilidade das transações e evitar o atingimento do

limite de *gas* por bloco da rede, o sistema segmenta automaticamente conjuntos superiores a 15 registros acadêmicos. Consequentemente, volumes maiores (cenários 3 e 4) demandam múltiplas transações sequenciais, o que introduz o custo fixo intrínseco de 21.000 unidades de *gas* para cada nova operação de rede, fator este devidamente considerado nas projeções financeiras apresentadas.

Tabela 5: Estimativa de custos totais na rede *Polygon* considerando a fragmentação por *chunks*

Métrica	Cenário 1	Cenário 2	Cenário 3	Cenário 4
Qtd. Estudantes	2	2	2	2
Qtd. Cursos	2	5	5	10
Qtd. Disciplinas	4	15	30	100
Qtd. Total de Notas	3	30	100	500
Nº de Transações (Chunks)	4	6	12	45
Custo Est. (POL)	0,0495	0,1320	0,3850	1,2540
Custo Est. (R\$)	0,0292	0,0680	0,2275	0,7411

Enquanto sistemas manuais apresentam uma curva de custo e tempo estritamente crescente, a arquitetura proposta demonstra que a eficiência do modelo de orquestração não apenas agiliza o fluxo administrativo, mas também torna a tecnologia blockchain acessível para instituições com grandes volumes de registros acadêmicos, mantendo a integridade e a segurança sem comprometer o orçamento institucional.

5.6 Discussão dos resultados

Os resultados obtidos confirmam que a descentralização da segurança, por meio da cifragem no lado do cliente, resolve o dilema entre transparência e privacidade em registros acadêmicos. A discussão central gira em torno da autonomia e soberania dos dados: ao implementar padrões criptográficos agnósticos (AES-256-GCM, PBKDF2 e ECIES), o sistema provou ser resiliente a mudanças tecnológicas externas e independente de bibliotecas proprietárias que poderiam limitar a interoperabilidade.

A introdução do serviço de orquestração com o *Apache Airflow* eliminou o gargalo operacional identificado no sistema-base. Enquanto a inserção manual de registros mostrava-se impraticável para volumes institucionais, a automação via arquivos CSV permitiu que o processamento de 500 notas (cenário 4) fosse realizado em apenas 42,1 segundos no ambiente *batch*. A inteligência do contrato em verificar a unicidade do conjunto (estudante, disciplina, semestre e ano) revelou-se um mecanismo crítico de integridade, impedindo registros redundantes ou

erros administrativos comuns em processos manuais.

Do ponto de vista econômico, a análise comparativa entre as redes foi reveladora. A transição da rede principal da *Ethereum* para a *Polygon* resultou em uma redução de custos de aproximadamente 99,9%, transformando um custo operacional de R\$ 81,43 (cenário 1) em apenas R\$ 0,03. Além disso, a estratégia de processamento em lote provou sua escalabilidade: no cenário 4, o custo por registro de nota caiu para frações de centavos, demonstrando que o custo fixo das transações blockchain é diluído de forma eficiente à medida que o volume de dados aumenta.

Por fim, a análise do desempenho da interface revelou que o tempo de cifragem no navegador (*DApp*), embora crescente com a carga, mantém-se dentro de limites aceitáveis de usabilidade, levando cerca de 58,5 segundos para processar 500 registros de alta sensibilidade. Isso valida o uso do PBKDF2 com alto número de iterações; o tempo despendido na derivação da chave é imperceptível diante da segurança adicional contra ataques de força bruta. Em geral, o equilíbrio entre a conveniência do processamento em massa e a economia transacional prova que a solução é tecnicamente superior aos modelos tradicionais e aos sistemas blockchain de primeira geração que careciam de uma camada de orquestração eficiente.

Capítulo 6

Conclusão

Este trabalho propôs e implementou uma arquitetura avançada para a gestão de registros acadêmicos em blockchain, posicionando-se como uma evolução direta e necessária ao trabalho base de [Pedrosa et al. \[2025\]](#). Enquanto a pesquisa anterior estabeleceu os fundamentos da descentralização acadêmica, este estudo introduziu contribuições críticas focadas em privacidade profunda, autonomia do usuário e, primordialmente, eficiência operacional para larga escala. Através do desenvolvimento de um serviço de orquestração baseado em *Apache Airflow* e de um modelo de criptografia híbrida, foi possível superar os gargalos de escalabilidade e as barreiras de segurança identificadas no modelo unitário original. A transição de um fluxo de inserção manual para um sistema automatizado de processamento em lote permitiu que centenas de registros fossem processados simultaneamente, garantindo uma redução drástica no esforço administrativo e uma economia financeira superior a 99% ao utilizar a rede *Polygon* em comparação à *mainnet* da *Ethereum*.

Ao implementar a cifragem no lado do cliente com o padrão ECIES e derivação de chaves via senha mestra, assegurou-se que informações sensíveis permaneçam inacessíveis a intermediários, mantendo o segredo criptográfico fora do alcance de servidores, uma melhoria significativa na arquitetura de privacidade em relação aos métodos anteriores. Conclui-se que a solução não apenas valida a viabilidade da tecnologia blockchain no setor educacional, mas estabelece um padrão de usabilidade institucional, provando que a orquestração de dados é o elo necessário para transformar modelos acadêmicos teóricos em ferramentas práticas e economicamente sustentáveis.

Como sugestões para trabalhos futuros, este sistema ainda pode ser aperfeiçoado. Em relação à segurança do contrato inteligente, a análise via *Cred Shield* aponta a oportunidade de otimizar o código para aumentar o *score* de proteção e eficiência, resolvendo vulnerabilidades e reduzindo ainda mais o consumo de *gas*. Para a interface do usuário, sugere-se a evolução da *DApp* visando uma experiência mais fluida (UX/UI), eliminando a fricção da cópia manual de endereços e integrando sistemas de *backup* em nuvem para chaves privadas cifradas, como o uso de provedores como *Google Drive* em substituição ao *download* local. Além disso, a

implementação de processos de *KYC* e a expansão do esquema de dados das entidades acadêmicas permitirão que o sistema suporte fluxos de informação mais densos e complexos. Por fim, vislumbra-se o uso de provas de conhecimento zero (*Zero-Knowledge Proofs*) para validação de competências, permitindo que a privacidade do egresso seja mantida mesmo em processos de verificação pública de diplomas e históricos.

Referências Bibliográficas

- Bom Dia Rio. Formandos da gama filho e univercidade, no rio, relatam problemas para conseguir os diplomas, 2019. URL <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/08/02/formandos-da-gama-filho-e-univercidade-no-rio-relatam-problemas-para-conseguir-os-diplomas-1.4812345.html>. Acessado em: 26 jan. 2026.
- Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform. https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf, 2014. White paper.
- Flavius. A word on secp256k1 and ecdsa. <https://www.flavius.io/media/a-word-on-secp256k1-and-ecdsa>, 2022. Acesso em: 11 jul. 2025.
- Constantinos Patsakis Fran Casino, Thomas K. Dasaklis. A systematic literature review of blockchain-based applications: Current status, classification and open issues, 2018.
- Ruizhe Jia and Steven Yin. To evm or not to evm: Blockchain compatibility and network effects. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security (DeFi'22)*. Association for Computing Machinery, 2022. doi: 10.1145/3560832.3563442. URL <https://doi.org/10.1145/3560832.3563442>.
- Yerlan Kistaubayev, Galimkair Mutanov, Madina Mansurova, Zhanna Saxenbayeva, and YasyNZhan Shakan. Ethereum-based information system for digital higher education registry and verification of student achievement documents. *Future Internet*, 15(1), 2023. ISSN 1999-5903. doi: 10.3390/fi15010003. URL <https://www.mdpi.com/1999-5903/15/1/3>.
- Dynamic Labs. Embedded wallets - dynamic. <https://www.dynamic.xyz/features/embedded-wallets>, 2024. Acesso em: 11 jul. 2025.
- Manisha Mali, Sakshi Aherkar, Prajwal Waykos, and Aishwarya Shukla. Blockchain-based academic bank of credit management system for higher education: An innovative approach to student credentialing and progression. In *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, pages 1–5, 2023. doi: 10.1109/ICBDS58040.2023.10346463.

- MetaMask. Metamask, 2025. URL <https://metamask.io>. Accessed: 29 June 2025.
- MetaMask Team. Metamask api method deprecation, 2023. URL <https://metamask.io/news/metamask-api-method-deprecation>. Acesso em: 22 jun. 2025.
- Ministério da Educação. Mec descredencia universidade gama filho e centro universitário da cidade. Disponível em <http://portal.mec.gov.br/component/tags/tag/univercidade>, 2014. [Acessado em 31/08/2024].
- Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, 2008. White paper.
- National Institute of Standards and Technology. Announcing the advanced encryption standard (aes). Federal Information Processing Standards Publication FIPS PUB 197, NIST, 2001.
- Sheela Rani P, Kaveri C, Nivedha M, Niveda S, Lakshi K, and Sandhiya R. A review on blockchain based security in education. In *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)*, pages 1122–1127, 2023. doi: 10.1109/ICPCSN58827.2023.00190.
- Bianca Pedrosa, Reissel de Souza, and Diogo Mendonça. Proof of concept for higher education academic record system using blockchain. In *Anais do VIII Workshop em Blockchain: Teoria, Tecnologias e Aplicações*, pages 29–42, Porto Alegre, RS, Brasil, 2025. SBC. doi: 10.5753/wblockchain.2025.8786. URL <https://sol.sbc.org.br/index.php/wblockchain/article/view/35465>.
- Abraham Silberschatz, Peter B. Galvin, and Greg Gagne. *Operating System Concepts*. John Wiley Sons, Hoboken, 10 edition, 2018.
- William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson, Boston, 7 edition, 2017.
- Shaik Arshiya Sultana, Chiramdasu Rupa, Ramanadham Pavana Malleswari, and Thippa Reddy Gadekallu. Ipfs-blockchain smart contracts based conceptual framework to reduce certificate frauds in the academic field. *Information*, 14(8):446, 2023. doi: 10.3390/info14080446. URL <https://www.mdpi.com/2078-2489/14/8/446>.
- Andrew S. Tanenbaum and Herbert Bos. *Modern Operating Systems*. Pearson, Boston, 4 edition, 2015.