De-Authorizer: Uma Arquitetura Baseada em Blockchain para Revogação Descentralizada de Acesso a Dados em Redes Sociais Online

Irvin S. Bezerra[1], **Valéria C. Times**[1], **Bruno N. Moreno**[2]

[1]Centro de Informática
Universidade Federal de Pernambuco (UFPE) – Recife – PE – Brazil

[2]Departamento de Sistemas e Computação
Instituto Federal de Tecnologia da Paraíba (IFPB) – Itabaiana – PB – Brazil

isb@cin.ufpe.br, vct@cin.ufpe.br, bruno.moreno@ifpb.edu.br

Abstract. *Online Social Networks (OSNs) centralize the control of personal data, hindering the revocation of consent as mandated by the GDPR and the LGPD. This paper presents De-Authorizer, a blockchain-based architecture that enables decentralized, auditable, and user-centric revocation of data access permissions. The proposal preserves the monetization models of OSNs and integrates smart contracts with Access Control Lists and OAuth 2.0. To ensure privacy and scalability, a hybrid (on-chain/off-chain) blockchain architecture is adopted. The architecture was developed following the Design Science Research Framework. Evaluation in a permissioned Proof of Authority network with up to 70.000 users achieved 3.214 TPS and an average latency of 7,75 s, demonstrating practical feasibility.*

Resumo. *Redes Sociais Online (RSO) centralizam o controle de dados pessoais, dificultando a revogação de consentimento exigida pelo GDPR e pela LGPD . Este trabalho apresenta o De-Authorizer, uma arquitetura baseada em blockchain para revogação descentralizada de acesso a dados, auditável e centrada no usuário. A proposta preserva os modelos de monetização das RSO e integra contratos inteligentes a ACLs e OAuth 2.0. Para garantir privacidade e escalabilidade, adota-se uma arquitetura de blockchain híbrida (on-chain/off-chain). A arquitetura foi desenvolvida segundo o Design Science Research Framework. A avaliação em rede permissionada Proof of Authority, com até 70.000 usuários, atingiu 3.214 TPS e 7,75 s de latência média, demonstrando viabilidade prática.*

1. Introdução

O crescimento das Redes Sociais *Online* (RSO) consolidou esses ambientes como principais mediadores do compartilhamento e do consumo de informações pessoais. Contudo, a centralização do armazenamento e do controle de dados nessas plataformas torna-as vulneráveis a incidentes de segurança e violações de privacidade. Casos amplamente divulgados, como o vazamento de 533 milhões de registros de usuários do *Facebook* em 2019 [Holmes 2021], evidenciam a dificuldade das RSO em assegurar governança adequada sobre dados sensíveis.

Em resposta a esses desafios, legislações como o *General Data Protection Regulation* (GDPR) e a Lei Geral de Proteção de Dados (LGPD) impuseram às organizações a

obrigação de garantir aos usuários, o direito de acesso, portabilidade e revogação do consentimento. Entretanto, o cumprimento efetivo desses direitos depende de mecanismos técnicos de controle que, em geral, permanecem sob domínio das próprias plataformas, limitando a autonomia dos usuários e a auditabilidade dos direitos do usuário.

As soluções atuais baseadas em *blockchain*, como as Redes Sociais *Online* descentralizadas (RSOD), oferecem transparência e imutabilidade, mas ainda apresentam limitações de interoperabilidade, escalabilidade e integração com RSO comerciais. Assim, persiste uma lacuna quanto a arquiteturas que permitam ao usuário, revogar seletivamente o acesso a seus dados, sem comprometer os modelos de monetização existentes.

Este trabalho propõe o *De-Authorizer*, uma arquitetura de software que utiliza contratos inteligentes na *blockchain Ethereum* para gerenciar e revogar permissões de acesso a dados de usuários em RSO compatíveis com *Access Control Lists* (ACLs) e *OAuth* 2.0. A proposta combina autenticação por provas de conhecimento-zero (PLONK) e armazenamento híbrido *on-chain*/*off-chain*, permitindo controle granular e auditável de consentimentos.

Até onde sabemos, não identificamos na literatura uma arquitetura que concilie, de forma integrada, (i) compatibilidade com RSO comerciais existentes, (ii) revogação seletiva e auditável de consentimentos diretamente pelo usuário, (iii) preservação dos modelos de monetização das plataformas e (iv) conformidade regulatória explícita com GDPR/LGPD por meio de contratos inteligentes. Nossa contribuição posiciona-se nesse espaço ao propor o *De-Authorizer* como uma arquitetura prática e interoperável para a revogação descentralizada de acesso em RSO já consolidadas.

O restante deste artigo está organizado da seguinte forma: a Seção 2 revisa os trabalhos relacionados; a Seção 3 descreve o problema, motivação e os objetivos e princípios de design; a Seção 4 descreve a arquitetura *De-Authorizer*; a Seção 5 apresenta o desenvolvimento da arquitetura *De-Authorizer*; a Seção 6 discute a avaliação experimental; e a Seção 7 apresenta as conclusões e perspectivas futuras.

2. Trabalhos Relacionados

A literatura recente demonstra o crescente interesse no uso de *blockchain* para controle de acesso e governança de dados distribuídos. Essa tecnologia, pela sua imutabilidade e auditabilidade, tem sido aplicada em diversos contextos, incluindo Internet das Coisas (IoT) [Pinno et al. 2017], privacidade em redes sociais [Guidi 2020, Mendoza-Tello et al. 2018] e rastreabilidade de dados [Wang et al. 2022]. No entanto, a adoção de *blockchain* como mecanismo de controle de acesso em Redes Sociais *Online* (RSO) ainda enfrenta desafios relacionados à escalabilidade, interoperabilidade e revogação seletiva de permissões.

As RSOD, como *SteemIt*[1] e *Sapien*[2], representam tentativas de substituir a centralização das RSO tradicionais por modelos baseados em *blockchain*. Essas plataformas, contudo, não permitem integração com RSO comerciais nem oferecem mecanismos para revogação granular de acesso, além de desconsiderarem os modelos de monetização existentes [Guidi 2020].

No campo dos mecanismos clássicos de controle, as *Access Control Lists* (ACLs)

[1] `https://steemit.com/`

[2] `https://www.sapien.network/`

continuam sendo amplamente utilizadas em sistemas computacionais [Li et al. 2017, Davari and Bertino 2019]. A combinação entre ACL e *blockchain* tem sido proposta como meio de reforçar a transparência e a rastreabilidade das permissões, mas as abordagens existentes permanecem limitadas quanto à interoperabilidade e à automação da revogação de consentimentos [Pinno et al. 2017].

Outros trabalhos exploram a integração entre *OAuth 2.0* e *blockchain* para delegação e auditoria de acesso distribuído. O trabalho de [Fotiou et al. 2019] propõe uma arquitetura descentralizada baseada em políticas de acesso, enquanto a proposta de [Mendoza-Tello et al. 2018] discutem modelos de privacidade reforçada, ambos sem integração nativa com RSO existentes. Já o *ControlChain* [Pinno et al. 2017] aplica *blockchain* ao domínio da IoT, com foco em rastreabilidade, mas sem suporte à revogação dinâmica de permissões. O framework proposto por [PRAVALLIKA et al. 2025] sugere gestão de permissões granular e armazenamento dos arquivos *on-chain*, porém não oferece suporte à integração com RSO já consolidadas.

A Tabela 1 sintetiza os principais trabalhos analisados, considerando quatro critérios recorrentes na literatura: (i) uso da *blockchain* como repositório de estados ou políticas de acesso; (ii) presença de mecanismos explícitos de governança; (iii) suporte à revogação de permissões; e (iv) avaliação de desempenho. A análise comparativa evidencia que, embora diversos trabalhos explorem governança e rastreabilidade, poucos oferecem suporte à revogação, e nenhum contempla simultaneamente revogação seletiva, interoperabilidade com RSO comerciais e avaliação de desempenho em cenários compatíveis com aplicações de larga escala.

Tabela 1: Estudos que utilizam *blockchain* para controle de permissões.

#	Autores	Critério 1	Critério 2	Critério 3	Critério 4
1	[Pinno et al. 2017]	✓	✓	-	-
2	[Li et al. 2017]	-	✓	✓	✓
3	[Mendoza-Tello et al. 2018]	-	✓	-	-
4	[Fotiou et al. 2019]	✓	-	-	✓
5	[Davari and Bertino 2019]	✓	✓	✓	-
6	[Yang et al. 2020]	✓	-	✓	-
7	[Guidi 2020]	✓	✓	-	✓
8	[Campanile et al. 2021]	✓	-	✓	-
9	[Zhang et al. 2021]	✓	✓	-	✓
10	[Wang et al. 2022]	✓	✓	-	-
11	[PRAVALLIKA et al. 2025]	✓	✓	-	-

Em síntese, a literatura revisada evidencia que nenhum dos trabalhos analisados oferece suporte à revogação seletiva e auditável de permissões de acesso em Redes Sociais *Online* já consolidadas. A maior parte das propostas concentra-se em aspectos de integridade, rastreabilidade ou delegação de acesso, tratando a revogação de forma limitada ou inexistente. Em particular, observa-se a ausência de mecanismos técnicos que operacionalizem o controle de consentimento exigido por legislações como a GDPR e a LGPD de maneira verificável, independente da plataforma e acionada diretamente pelo usuário. Essa lacuna consiste em uma das motivações principais para o desenvolvimento

do trabalho aqui proposto.

Além disso, embora algumas abordagens explorem governança e auditoria por meio de *blockchain*, as soluções por elas propostas não contemplam simultaneamente interoperabilidade com mecanismos amplamente adotados em RSO comerciais, como *Access Control Lists* (ACLs) e *OAuth* 2.0, nem consideram explicitamente a preservação dos modelos econômicos e operacionais dessas plataformas. Essa lacuna motiva a necessidade de uma abordagem arquitetural que permita a revogação descentralizada e auditável de consentimentos, sem exigir a substituição das infraestruturas existentes, conforme discutido na seção seguinte.

3. Problema e Metodologia

O gerenciamento centralizado dos dados dos usuários em RSO impõe sérios desafios à privacidade e à governança das informações. Apesar da existência de legislações como o GDPR[3] e a LGPD[4], que asseguram direitos fundamentais como acesso, correção, eliminação e revogação de consentimento, a implementação técnica desses direitos ainda é incipiente. As RSO mantêm mecanismos proprietários e heterogêneos, o que limita a autonomia dos usuários e dificulta a rastreabilidade de ações de revogação e consentimento.

Para investigar esse problema de forma sistemática e orientar a concepção de uma solução técnica, este trabalho adota o *Design Science Research Framework* (DSRF) [Peffers et al. 2007]. O DSRF estrutura a pesquisa em quatro etapas principais: (*i*) identificação do problema; (*ii*) definição dos objetivos da solução; (*iii*) design e desenvolvimento do artefato; e (*iv*) implementação da proposta e avaliação de seus resultados. As duas primeiras etapas são detalhadas nesta seção, enquanto as etapas de design do artefato e de aplicação da proposta são apresentadas, respectivamente, na Seção 4 e na Seção 5.

3.1. Identificação do Problema e Motivação

A etapa inicial do DSRF consistiu em identificar os principais desafios enfrentados por usuários de RSO quanto ao controle de seus dados pessoais. Para isso, foi conduzido um questionário *online* entre 27 de setembro e 17 de outubro de 2022, com 45 respondentes dos estados de Pernambuco, Paraíba, Alagoas e Rio Grande do Norte. Embora a amostra seja limitada e não permita inferência estatística ou generalização, ela foi suficiente para uma análise exploratória inicial, evidenciando indícios das dificuldades percebidas pelos usuários no exercício de seus direitos. Assim, o questionário tem caráter estritamente exploratório, servindo apenas para contextualização do problema.

Os resultados, resumidos na Tabela 2, revelam que, embora 55,6% dos participantes afirmem conhecer a LGPD, apenas 15,6% conseguiram recuperar dados comprometidos e nenhum considerou simples o processo de solicitação. Isso indica que, apesar da conscientização crescente sobre privacidade, o exercício efetivo desses direitos permanece um desafio técnico e operacional significativo nas RSO.

[3] https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Tabela 2: Percepção dos usuários sobre danos e recuperação de dados em RSO.

Questão	Respostas "Sim"
Canal simples para reclamação ou recuperação de dados	15,6%
Ação de recuperação eficaz	15,6%
Facilidade para requisitar auxílio	0,0%
Ocorrência de danos financeiros ou morais	2,2%
Conhecimento sobre a LGPD	55,6%

Essas evidências fundamentaram a formulação dos seguintes *Design Requirements* (DRs), que definem as condições necessárias para o desenvolvimento de uma solução técnica capaz de garantir o controle de acesso e revogação de dados em conformidade com a LGPD:

DR#1: As garantias de revogação do acesso aos dados do usuário devem ser implementadas por um sistema que incorpore as legislações vigentes, como o GDPR e a LGPD;

DR#2: As funcionalidades de revogação, desautorização e monitoramento de acesso devem estar integradas em uma plataforma unificada, acessível e auditável pelo usuário final.

3.2. Definição dos Objetivos e Princípios de Projeto

Com base nos requisitos identificados, a segunda etapa do DSRF estabelece os *Design Principles*. Cada princípio está diretamente associado a um requisito e traduz a necessidade legal em uma solução técnica viável.

DP#1: Controle Unificado: as operações de autorização, revogação e monitoramento devem ser consolidadas em um ponto único de controle, facilitando a gestão pelo usuário;

DP#2: Revogação Descentralizada: as solicitações de desautorização devem ser executadas diretamente pelo usuário por meio de contratos inteligentes (*smart contracts*), eliminando a dependência da RSO para efetivação de desautorização;

DP#3: Privacidade Criptográfica: a proteção dos dados e o registro das operações de acesso e revogação devem ser assegurados por mecanismos de criptografia e embaralhamento, garantindo confidencialidade e auditabilidade.

Esses princípios convergem para uma abordagem que une conformidade regulatória e viabilidade tecnológica. A tecnologia *blockchain*, por meio do uso de contratos inteligentes, oferece o ambiente adequado para codificar e automatizar tais garantias. Assim, o *De-Authorizer* implementa esses princípios de projeto, promovendo um modelo descentralizado, auditável e tecnicamente escalável de gestão de consentimentos, detalhado na Seção 4.

4. Arquitetura Proposta: De-Authorizer

Esta seção apresenta a arquitetura *De-Authorizer*, codificada seguindo os princípios de projeto estabelecidos na Seção 3.2 — controle unificado **(DP#1)**, revogação descentralizada **(DP#2)** e privacidade criptográfica **(DP#3)**.

4.1. Visão Geral e Motivação Arquitetural

No modelo de negócios vigente, o armazenamento de dados e o controle de permissões de acesso são integralmente centralizados nas RSO. Esse arranjo limita a autonomia do usuário, dificulta a revogação efetiva de permissões, especialmente em cenários de incidentes de segurança ou uso indevido de dados e ainda permite a reutilização e retenção de conteúdo mesmo após o encerramento de contas [Bataineh et al. 2020, Shukla et al. 2023].

O *De-Authorizer*, conforme ilustrado na Figura 1, atua como uma camada intermediária entre o usuário, as RSO e a *blockchain*, explicitando os fluxos de autorização, verificação e revogação de permissões. Diferentemente do modelo de negócios tradicional, o controle de permissões deixa de ser exclusivamente centralizado nas RSO, passando a ser registrado e auditado por meio de eventos imutáveis em contratos inteligentes. Nesse arranjo, os dados continuam armazenados nas RSO, preservando seus modelos de monetização, enquanto a *blockchain* mantém apenas metadados e estados de autorização, permitindo revogação explícita, verificável e iniciada pelo usuário.

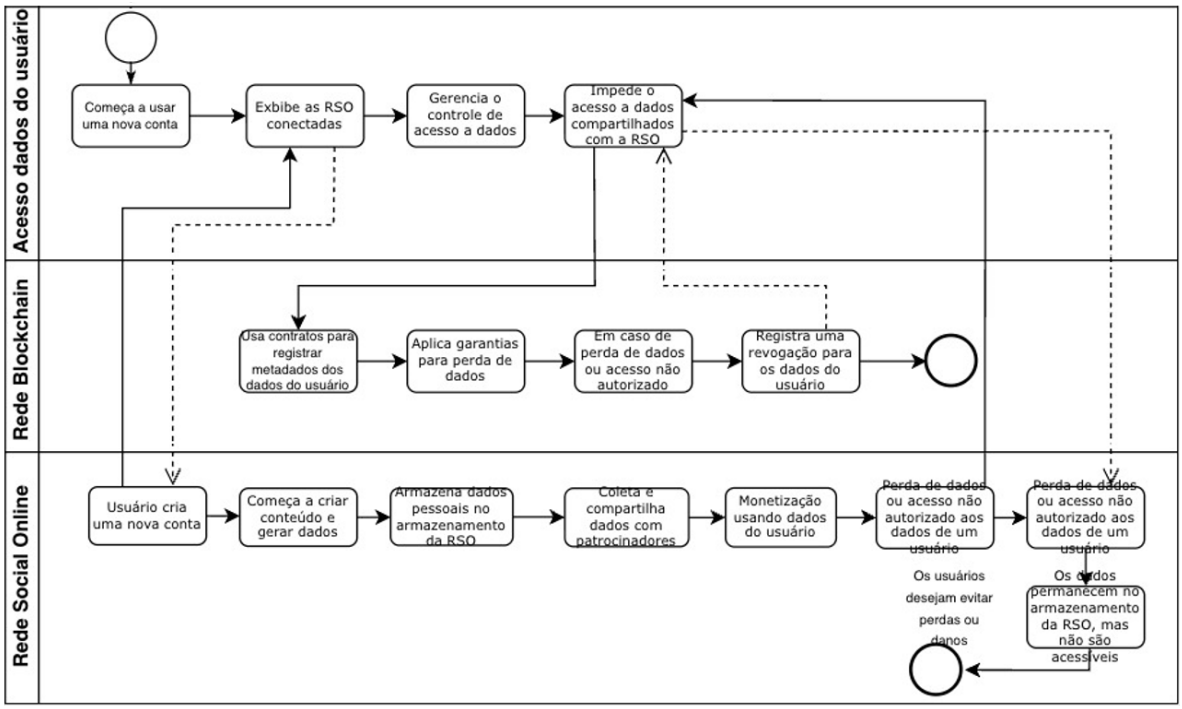

Figura 1: Modelo de negócios proposto com a introdução do *De-Authorizer* (*TO-BE*).

4.2. Arquitetura Conceitual e Componentes Principais

A arquitetura é implementada sobre uma rede compatível com a máquina virtual do *Ethereum*, utilizando a linguagem *Solidity* para construção de contratos inteligentes, escolhida por sua ampla adoção e pela baixa curva de aprendizado [Zhang et al. 2021]. A Figura 2 apresenta a visão de alto nível do *De-Authorizer*, composto pelos seguintes contratos e camadas de apoio:

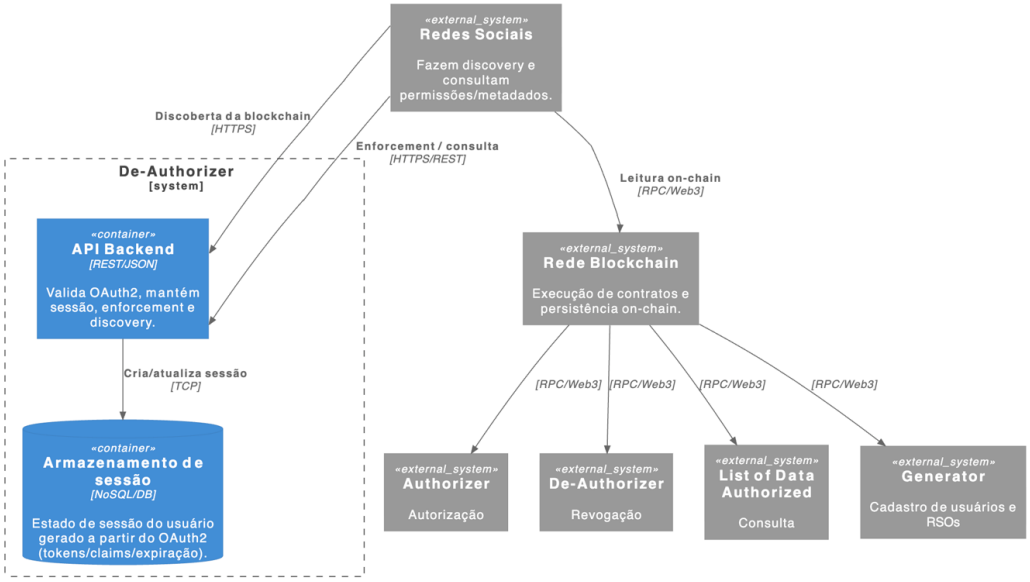

Figura 2: Diagrama de arquitetura do *De-Authorizer*.

- **Generator** — contrato base que mantém o estado e os *metadados* de permissões (lista de autorizações e revogações), além do cadastro de usuários e RSO;
- **Authorizer** — provê funções para criação/atualização de permissões (autorização);
- **De-Authorizer** — provê funções para *revogação* de permissões (desautorização);
- **List of Data Authorized** — oferece leitura pública do estado das permissões, para consumo por RSO e auditores;
- **Camada de Identidade e Integração** — serviços *off-chain* (*OAuth* 2.0, *DApp* e *API*) que unem RSO, usuários e contratos inteligentes.

Os contratos especializados (*Authorizer*, *De-Authorizer* e *List of Data Authorized*) acessam o estado mantido pelo contrato *Generator*, promovendo encapsulamento, separação de responsabilidades, organização e padronização.

4.3. Contratos Inteligentes e Fluxo de Operações

Esta subseção descreve os contratos inteligentes e o fluxo operacional do *De-Authorizer*, enfatizando suas especializações funcionais. Em conjunto com a Subseção 4.4, estabelece mecanismos auditáveis de autorização e revogação, integrando autenticação *off-chain* e rastreabilidade *on-chain*.

Papel dos contratos: *Generator* armazena *metadados* essenciais (endereço do usuário na *blockchain*, RSO, identidade digital do dado, situação e data/hora). *Authorizer* registra autorizações; *De-Authorizer* registra revogações; e o *List of Data Authorized* disponibiliza consulta pública do estado (permitido/revogado) por par (usuário, RSO, dado).

Autorização e autenticação (*Authorizer*): A autenticação ocorre predominantemente *off-chain*, em que o usuário comprova a posse ou associação a um dado por meio de uma identidade digital derivada de funções de *hash* (Keccak-256 *on-chain*) e do contexto de uso (por exemplo, RSO e escopo). Opcionalmente, *De-Authorizer* é compatível com o uso de provas de conhecimento zero, como PLONK [Gabizon et al. 2019, Fiege et al. 1987], um protocolo que permite verificar propriedades sobre dados sem a necessidade de revelá-los, reforçando garantias de privacidade sem

alterar o fluxo principal de autorização. O resultado da autorização é então registrado *on-chain* pelo contrato *Authorizer*.

Revogação (*De-Authorizer*): A revogação consiste em uma transição explícita de estado, acionada diretamente pelo usuário por meio de seu endereço na *blockchain*. Essa operação invalida o direito de acesso previamente concedido, sem implicar a exclusão do dado, e gera um evento imutável que possibilita auditoria posterior.

Listagem e auditoria (*List of Data Authorized*): Fornece operações de leitura para as RSO validarem, em tempo de uso, se um acesso permanece permitido. Para mitigar riscos de abuso, cada permissão é vinculada à RSO de origem; logo, uma RSO não obtém permissões alheias ao seu escopo.

4.4. Mecanismos de Identidade, Armazenamento e Privacidade

Identidade e *OAuth* 2.0: A camada *off-chain* integra-se aos provedores de identidade das RSO via *OAuth* 2.0[5], permitindo vincular contas (e.g. e-mail/perfil) ao endereço do usuário na *blockchain* (carteira digital). Esse vínculo é mantido em repositório *NoSQL* com criptografia de dados em repouso.

Armazenamento híbrido (*on-chain*/*off-chain*): A *blockchain* armazena exclusivamente *metadados* e eventos de controle de acesso; nenhum dado pessoal bruto é registrado *on-chain*. Identificadores e carimbos de data e hora são derivados por funções de embaralhamento criptográfico, combinadas com valores aleatórios (*salt*) e secretos (*pepper*) mantidos *off-chain*, reduzindo riscos de *linkability* (correlação indevida entre registros) e ataques de dicionário.

Privacidade e ZKP: Quando aplicável, o *De-Authorizer* prevê o uso de provas de conhecimento zero, como o protocolo PLONK [Gabizon et al. 2019], como um mecanismo complementar de privacidade na arquitetura. Esse recurso permite comprovar conhecimento ou posse de determinados dados sem a necessidade de revelá-los, reduzindo a exposição de informações sensíveis durante o processo de autorização. A execução do verificador ZKP pode ocorrer de forma *off-chain*, com o resultado ancorado na *blockchain* para fins de auditabilidade. Dessa forma, o uso de ZKP é proposto como extensão da arquitetura, contribuindo para a ampliação das capacidades de privacidade da arquitetura, ainda que sua avaliação completa seja tratada como trabalho futuro.

4.5. Integração com RSO e *API* de Acesso

As RSO interagem com o *De-Authorizer* por meio de uma *API* padronizada que estende os mecanismos tradicionais de introspecção e revogação de tokens do *OAuth* 2.0 e ACLs. Para mitigar gargalos de latência em tempo de execução, a arquitetura adota uma estratégia híbrida: as plataformas realizam a validação contínua dos escopos localmente por meio de estruturas de cache *off-chain*. Esse cache local é invalidado de forma reativa a partir da escuta de eventos assíncronos e imutáveis gerados pelo contrato *List of Data Authorized* quando ocorre uma revogação. Assim, o *De-Authorizer* opera como uma camada complementar de governança e auditoria regulatória, fornecendo verificabilidade enquanto minimiza impactos na escalabilidade e no desempenho operacional de acesso das RSO.

O mecanismo de *enforcement* combina: (i) *APIs* autenticadas e auditáves, e (ii) SLA que definem metas de disponibilidade, latência e conformidade. Um *Decentralized*

[5] `https://datatracker.ietf.org/doc/html/rfc6749`

Application (*DApp*) realiza a ponte entre a interface *web*, as carteiras dos usuários e os contratos, viabilizando a operação ponta a ponta conforme apresentado na Figura 2.

Em síntese, a arquitetura implementa os DPs mapeando: identidade e autorização (**DP#1**), transições explícitas de estado para revogação (**DP#2**) e proteção/anonimização de identificadores e eventos (**DP#3**). A Seção 6 apresenta e discute os resultados de desempenho e escalabilidade.

5. Implementação e Cenário Experimental

A quarta etapa do DSRF compreende a implementação e avaliação do artefato, descrevemos como o protótipo *De-Authorizer* foi implementado. A análise crítica dos resultados é apresentada na Seção 6.

Ambiente de Implementação e Ferramentas: O *De-Authorizer* foi implementado na *blockchain* compatível com a *Ethereum Virtual Machine* (EVM), utilizando *Solidity* para a programação dos contratos inteligentes. O cliente de nó empregado foi o *Geth*, configurado com consenso *Proof of Authority (PoA)* em cinco nós validadores. Para fins de mensuração, foi usada a ferramenta de *benchmark BlockCompass*[6], que gera cargas de transações e coleta indicadores de desempenho.

Para isolar o comportamento do artefato de custos econômicos de redes públicas, adotou-se custo de GAS igual a 0, política de confirmação em todos os blocos e uma *thread* por minerador. O *DApp* integra a interface *web* aos contratos, permitindo a execução ponta a ponta dos fluxos avaliados. Os experimentos foram executados no Ubuntu 18.04 (64 bits) sobre processador Intel Core i5-10500T, com 8 GB de memória RAM e armazenamento SSD NVMe.

Contratos e Funções Avaliadas: A avaliação concentrou-se nos contratos *Generator* e *De-Authorizer* por estes representarem operações centrais no fluxo de uso do sistema. Em particular, foram analisadas as funções *newUser*, responsáveis pelo registro inicial de usuários, e *deDataUsr*, responsável pela revogação explícita de permissões de acesso. Na revogação, o mecanismo de autenticação baseado em provas criptográficas é abstraído por um valor booleano, permitindo avaliar o impacto da operação sem introduzir complexidade adicional no experimento.

Cenários de Carga e Geração de Dados: Foram definidos três cenários de carga, correspondentes a diferentes ordens de grandeza no número total de usuários: leve (700 usuários), médio (7.000 usuários) e amplo (70.000 usuários). Esses cenários visam representar padrões progressivos de crescimento típicos de plataformas sociais, permitindo observar o comportamento do sistema.

Os dados foram gerados de forma sintética e aleatória pelo *BlockCompass*, evitando efeitos de cache ou padrões artificiais de acesso. As transações foram emitidas em lotes com intervalo fixo de 10 segundos, com distribuição aleatória intra lote, até que o volume correspondente a cada cenário fosse atingido.

Métricas e Procedimento de Medição: A metodologia adotada baseia-se em mensuração orientada a transações, contabilizando todas as transações emitidas, independentemente de sucesso ou falha, a fim de evitar distorções decorrentes de descarte silencioso. As métricas coletadas incluem: (i) vazão de transações por segundo (TPS);

[6] `https://github.com/irvin-s/de_auth_benchmark`

(ii) latência média por transação; (iii) uso percentual de CPU e memória; e (iv) volume de tráfego de rede. Valores extremos que resultaram em erro total de execução foram descartados da estatística sumária. Para cada cenário são reportadas médias agregadas, utilizadas como base para a análise comparativa apresentada posteriormente.

Limitações e Considerações Econômicas: Os experimentos foram conduzidos em uma rede privada com consenso *PoA* e custo de GAS igual a zero, não refletindo diretamente os custos financeiros e a variabilidade de latência observados em redes públicas não permissionadas. Embora essa escolha permita avaliar o comportamento funcional e de desempenho do *De-Authorizer* de forma controlada, ela limita a generalização direta dos resultados para cenários públicos.

Como extensão natural, considera-se a adoção de arranjos de consórcio nos quais RSO e provedores de identidade compartilham a validação sob modelos de governança definidos, preservando previsibilidade de custos e níveis de serviço.

6. Resultados e Discussão

Nesta seção são discutidos o desempenho obtido em diferentes cenários de carga, sua comparação com soluções existentes e as implicações técnicas. A Tabela 3 sintetiza os resultados médios para as três cargas de trabalho — leve, média e ampla — geradas pelo *benchmark BlockCompass*. Observa-se comportamento consistente de escalabilidade, com crescimento linear no volume de transações processadas e aumento previsível da latência à medida que o número de usuários cresce.

No cenário de 70.000 usuários, considerado o mais representativo para ambientes de produção, foram registradas 3.214 transações por segundo (TPS) e latência média de 7,75 s. Esse valor representa um desempenho significativamente superior ao de redes *blockchain* baseadas em consenso *Proof of Work* (PoW), cuja taxa média situa-se em torno de 80 TPS [Gramoli et al. 2023], e competitivo com resultados recentes obtidos por arquiteturas otimizadas, as quais alcançam cerca de 243 TPS [Camilo et al. 2022].

A latência média de 7,75 segundos observada na liquidação *on-chain* do cenário amplo (70.000 usuários) poderia afetar a usabilidade caso a operação fosse tratada de forma síncrona e bloqueante na interface. Nesse contexto, a operação pode ser implementada por meio de uma arquitetura assíncrona, na qual o usuário submete a requisição de revogação de acesso, recebe uma confirmação imediata de envio do protocolo pela aplicação e pode continuar utilizando a plataforma normalmente enquanto a transição de estado é minerada e confirmada na *blockchain* em segundo plano.

Tabela 3: Sumário de resultados por carga (médias)

Tipo	Total de usuários	Tempo de execução	Usuários (méd)	Transações/s	Latência
Leve	700	00:09:40	361	1.703	0,01 s
Médio	7.000	00:09:45	4.433	1.822	2,5 s
Amplo	70.000	00:38:25	43.166	3.214	7,75 s

A utilização moderada de CPU (14,06%) e memória (7,17%) indica boa eficiência na execução das operações de validação e na interação entre os contratos inteligentes construídos. Essa eficiência decorre do uso do consenso *Proof of Authority (PoA)*, que

reduz a complexidade computacional associada à mineração de blocos, tornando o sistema mais adequado a ambientes corporativos permissionados, como RSO comerciais. O tráfego de rede observado — 4,76 GB de entrada e 2,87 GB de saída — é compatível com a alta densidade transacional e sugere potencial para implantação em redes distribuídas de médio porte.

Para fins de contextualização operacional, redes sociais de grande escala, como a plataforma X, operam com volumes médios da ordem de milhares de eventos por segundo, atingindo picos significativamente maiores em eventos excepcionais[7]. Nesse sentido, os valores obtidos pelo *De-Authorizer* situam-se na mesma ordem de grandeza de operação contínua de RSO reais, servindo como referência de viabilidade e não como equivalência funcional direta.

6.1. Discussão Comparativa com o Estado da Arte

A análise comparativa considera três classes de abordagens: (i) o estado da prática adotado por RSO comerciais, baseado em *OAuth* 2.0 e listas de controle de acesso centralizadas; (ii) propostas clássicas de autorização descentralizada baseadas em *blockchain*, como ControlChain [Pinno et al. 2017]; e (iii) trabalhos recentes focados em preservação de privacidade em redes sociais, como RecGuard [Frimpong et al. 2023].

Soluções tradicionais baseadas em *OAuth* 2.0 oferecem ampla adoção e maturidade industrial, porém mantêm o controle de revogação concentrado nas plataformas, limitando a autonomia do usuário. Abordagens baseadas em *blockchain*, como ControlChain, introduzem descentralização, mas pressupõem armazenamento e controle totalmente distribuídos, o que dificulta a integração com RSO existentes. Trabalhos recentes em privacidade, como RecGuard, concentram-se na proteção do conteúdo, sem abordar de forma explícita a revogação auditável de permissões.

Outras propostas baseadas em rastreabilidade em nuvem [Wang et al. 2022] continuam dependentes de provedores centralizados, enquanto modelos totalmente descentralizados [PRAVALLIKA et al. 2025] apresentam baixa compatibilidade com ecossistemas comerciais consolidados. Normas e relatórios institucionais, como o NIST IR 8403 [Hu and Hu 2022], reforçam a necessidade de soluções que conciliem descentralização seletiva, auditabilidade e interoperabilidade.

Não foi utilizado um baseline experimental diretamente comparável, pois as soluções existentes não combinam simultaneamente revogação seletiva, integração com RSO, *OAuth*/ACL e avaliação em *blockchain* permissionada. Trabalhos relacionados foram usados apenas como referência contextual de desempenho, e não como base comparativa direta.

Nesse contexto, o *De-Authorizer* diferencia-se ao oferecer revogação explícita e verificável de permissões, preservando a infraestrutura e os modelos de monetização das RSO, o que o posiciona de forma complementar às soluções existentes.

6.2. Implicações e Síntese dos Resultados

Os resultados obtidos evidenciam que o *De-Authorizer* não apenas mantém compatibilidade com o modelo econômico das RSO, mas também amplia a governança do usuário sobre seus dados pessoais — um requisito central das legislações de privacidade contemporâneas. A arquitetura permite que a revogação de acesso seja executada diretamente

[7] https://blog.x.com/engineering/en_us/a/2013/new-tweets-per-second-record-and-how

pelo titular dos dados, sem intervenção da plataforma, o que representa um avanço em direção à autodeterminação informacional.

Do ponto de vista computacional, a capacidade de processamento observada revela que soluções de controle de permissões baseadas em *blockchain* podem atingir níveis de desempenho compatíveis com aplicações de grande escala, desde que adotem estratégias híbridas (*on-chain*/*off-chain*) e consensos leves, como o *PoA*. Já do ponto de vista regulatório, a integração com *OAuth 2.0* e ACLs viabiliza a adoção progressiva do *De-Authorizer* sem ruptura com as infraestruturas computacionais existentes.

Do ponto de vista da segurança da informação, o modelo de ameaças considerado inclui: (i) plataformas sociais maliciosas ou negligentes, capazes de abusar de fluxos de autorização; (ii) coleta automatizada de dados por meio de *scrapers*, isto é, agentes automatizados que realizam coleta massiva de dados por meio de *API*s ou interfaces públicas; (iii) abuso interno de privilégios; e (iv) observadores *on-chain* interessados em inferir vínculos entre usuários e dados. A identificação dessas ameaças foi orientada pelos modelos STRIDE e LINDDUN.

As principais mitigações adotadas envolvem minimização e pseudonimização de dados, autenticação realizada fora da *blockchain*, uso de *APIs* padronizadas com controles de acesso explícitos e acordos de nível de serviço auditáveis. Técnicas criptográficas, como funções de *hash* combinadas com valores aleatórios (*salt*) e secretos (*pepper*) mantidos *off-chain*, reduzem riscos de correlação indevida e ataques de dicionário. A prevenção de ataques de repetição e *Sybil* (criação massiva de identidades falsas) é reforçada pelo uso de *nonce* único por transação, conforme a especificação EIP-155, que contribui para a distinção de domínios de transação e para a mitigação de reexecuções indevidas.

Portanto, o *De-Authorizer* contribui em quatro dimensões: (i) arquitetural, ao propor uma solução integrada que combina contratos inteligentes, *OAuth* 2.0, ACLs e armazenamento híbrido para viabilizar a revogação descentralizada e auditável de permissões; (ii) técnica, ao demonstrar escalabilidade e eficiência por meio de avaliação experimental; (iii) conceitual, ao redefinir a relação entre controle de dados e monetização em RSO; e (iv) regulatória, ao oferecer suporte à conformidade com legislações como GDPR e LGPD. Esses resultados indicam o potencial da proposta para cenários de revogação descentralizada de acesso a dados em ambientes distribuídos.

7. Conclusão e Trabalhos Futuros

Este trabalho apresentou o ***De-Authorizer***, uma arquitetura baseada em *blockchain* permissionada e contratos inteligentes voltada à revogação descentralizada e auditável de autorizações de acesso a dados pessoais em RSO. A proposta foi concebida e avaliada segundo a metodologia *Design Science Research Framework* (DSRF), materializando três princípios de projeto: controle unificado de consentimento, revogação descentralizada e preservação de privacidade por mecanismos criptográficos.

A avaliação experimental mostrou que *De-Authorizer* sustenta **3.214** TPS com latência média inferior a **7,75** segundos em um ambiente com cinco nós validadores, indicando viabilidade para RSO de larga escala. Como trabalhos futuros, destacam-se a avaliação da arquitetura em ambientes de consórcio com múltiplas RSO, a validação da proposta em cenários reais com integração a plataformas existentes, a análise de custos e desempenho em redes públicas ou híbridas, e a incorporação de mecanismos avançados de prova de conhecimento zero para fortalecer garantias de privacidade.

Referências

Bataineh, A. S., Mizouni, R., Bentahar, J., and El Barachi, M. (2020). Toward monetizing personal data: a two-sided market analysis. *Future Generation Computer Systems*, 111:435–459.

Camilo, G. F., Campista, M. E. M., Costa, L. H. M., and Duarte, O. C. M. (2022). Disponibilizaçao segura, automática e confiável de dados proprietários utilizando corrente de blocos. *Revista Eletrônica de Iniciação Científica em Computação*, 20(3).

Campanile, L., Iacono, M., Marulli, F., and Mastroianni, M. (2021). Designing a gdpr compliant blockchain-based iov distributed information tracking system. *Information Processing & Management*, 58(3):102511.

Davari, M. and Bertino, E. (2019). Access control model extensions to support data privacy protection based on gdpr. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 4017–4024. IEEE.

Fiege, U., Fiat, A., and Shamir, A. (1987). Zero knowledge proofs of identity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 210–217.

Fotiou, N., Pittaras, I., Siris, V. A., Voulgaris, S., and Polyzos, G. C. (2019). Secure iot access at scale using blockchains and smart contracts. In *2019 IEEE 20th International Symposium on"A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pages 1–6. IEEE.

Frimpong, S. A., Han, M., Boahen, E. K., Sosu, R. N. A., Hanson, I., Larbi-Siaw, O., and Senkyire, I. B. (2023). Recguard: An efficient privacy preservation blockchain-based system for online social network users. *Blockchain: Research and Applications*, 4(1):100111.

Gabizon, A., Williamson, Z. J., and Ciobotaru, O. (2019). Plonk: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. *Cryptology ePrint Archive*.

Gramoli, V., Guerraoui, R., Lebedev, A., Natoli, C., and Voron, G. (2023). Diablo: A benchmark suite for blockchains. In *Proceedings of the Eighteenth European Conference on Computer Systems*, pages 540–556.

Guidi, B. (2020). When blockchain meets online social networks. *Pervasive and Mobile Computing*, 62:101131.

Holmes, A. (2021). 533 million facebook users' phone numbers and personal data have been leaked online.

Hu, V. C. and Hu, V. C. (2022). *Blockchain for access control systems*. US Department of Commerce, National Institute of Standards and Technology.

Li, R., Shen, C., He, H., Gu, X., Xu, Z., and Xu, C.-Z. (2017). A lightweight secure data sharing scheme for mobile cloud computing. *IEEE Transactions on Cloud Computing*, 6(2):344–357.

Mendoza-Tello, J. C., Mora, H., Pujol-López, F. A., and Lytras, M. D. (2018). Social commerce as a driver to enhance trust and intention to use cryptocurrencies for electronic payments. *Ieee Access*, 6:50737–50751.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77.

Pinno, O. J. A., Gregio, A. R. A., and De Bona, L. C. (2017). Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–6. IEEE.

PRAVALLIKA, G., RAO, C. P., and DEEPIKA, Y. V. S. (2025). A block chain-based security sharing framework with fine-grained access control for personal data. *Stanford & Oxbridge Journal of Emerging Science and Computing Intelligence (SOJ-ESCI)*, 5(2):29–37.

Shukla, S., Bisht, K., Tiwari, K., and Bashir, S. (2023). *Data Economy in the Digital Age*. Springer.

Wang, Y., Li, S., Liu, H., Zhang, H., and Pan, B. (2022). A reference architecture for blockchain-based traceability systems using domain-driven design and microservices. In *2022 29th Asia-Pacific Software Engineering Conference (APSEC)*, pages 269–278. IEEE.

Yang, F., Wang, Y., Fu, C., Hu, C., and Alrawais, A. (2020). An efficient blockchain-based bidirectional friends matching scheme in social networks. *IEEE Access*, 8:150902–150913.

Zhang, S., Yao, T., Arthur Sandor, V. K., Weng, T.-H., Liang, W., and Su, J. (2021). A novel blockchain-based privacy-preserving framework for online social networks. *Connection Science*, 33(3):555–575.