Mensageria Descentralizada como Infraestrutura Pública

Uma Perspectiva sobre a Web3 como Bem Comum Digital

Fabrício Barbosa Viegas
Universidade Federal de Pelotas
Pelotas, Rio Grande do Sul
fbviegas@inf.ufpel.edu.br

Murilo Costa Salem
Universidade Federal de Pelotas
Rio Grande do Sul, Brasil
mcsalem@inf.ufpel.edu.br

Tatiana Aires Tavares
Universidade Federal de Pelotas
Rio Grande do Sul, Brasil
tatiana@inf.ufpel.edu.br

ABSTRACT

Digital messaging plays a central role in modern society, but it is currently dominated by centralized platforms that compromise user privacy and control. This position paper argues that decentralized messaging systems, based on open protocols and free software, can serve as public communication infrastructure and exemplify Web3 as a digital common good. We discuss the limitations of current services (identity lock-in, user fragmentation, data exposure) and present decentralized approaches (peer-to-peer, federated, blockchain-based) according to recent literature. We relate these models to the concept of public digital infrastructure, essential communication systems managed in a non-exclusive manner, and the notions of digital commons. As illustrative cases, we cite open protocols like Matrix and Web3 initiatives that adopt blockchain-based identity (e.g., XMTP), showing that such systems exhibit the characteristics of common resources: public specification, collective governance, and open-source software.

KEYWORDS

mensageria descentralizada, infraestrutura pública digital, Web3, bens comuns digitais, software livre

1 INTRODUÇÃO

Na era da Web3, cresce a demanda por serviços digitais que funcionem como bens públicos. A comunicação online é fundamental para a vida social e econômica contemporânea, mas ainda hoje se baseia na maioria em plataformas fechadas e privadas (e.g. WhatsApp, Telegram, Messenger...). Tais sistemas centralizados impõem riscos significativos: usuários perdem controle sobre seus dados, tornando-os vulneráveis à censura e vigilância. Como observa Yeung [15], "a comunicação é a espinha dorsal do mundo digital, e sua centralização implica riscos significativos… especialmente em termos de privacidade, segurança e soberania dos dados". Além disso, a dependência de poucas empresas leva a casos de banimento arbitrário de contas e fragmentação de identidade – cada usuário precisa manter múltiplas contas em serviços diferentes, dificultando a interoperabilidade.

Por outro lado, a Web3 surge com a promessa de tecnologias descentralizadas como blockchain, redes peer-to-peer e protocolos abertos, que permitem um novo paradigma de serviços colaborativos. A literatura sobre bens digitais comuns aponta exemplos exitosos de recursos globais geridos por comunidades, como o software livre e a Wikipédia[10]. Nesse contexto, propõe-se que a mensageria descentralizada seja vista como um bem comum digital e tratada como infraestrutura pública de comunicação. Isto significa projetar e implementar sistemas de mensagens abertos, baseados em software livre e governança distribuída, visando maximizar o bem público. A tabela 1, demonstra como podemos analisar abordagens técnicas como Peer-to-Peer (P2P), Federação e Blockchain para mensageria descentralizada e conectarmos esses conceitos à teoria de infraestrutura digital.

2 METODOLOGIA

A abordagem metodológica adotada neste trabalho é de caráter qualitativo e exploratório, buscando articular conceitos de infraestrutura digital pública, bens comuns digitais e tecnologias de mensageria descentralizada com estudos de caso contemporâneos. O objetivo foi compreender de que maneira a centralização da comunicação em plataformas privadas impacta a soberania digital e quais alternativas podem ser construídas como serviços essenciais.

O percurso metodológico desenvolveu-se em três frentes complementares. Em primeiro lugar, realizou-se uma revisão bibliográfica e documental, abrangendo literatura acadêmica, relatórios técnicos, fontes jornalisticas para levantamento da opinião pública sobre o assunto e documentos de organismos internacionais sobre infraestrutura digital, Web3 e mensageria descentralizada, bem como referenciais teóricos acerca de bens comuns digitais e soberania tecnológica. Por fim, procedeu-se à análise de iniciativas governamentais de mensageria pública em diferentes países, incluindo França, Alemanha, OTAN/EUA e Brasil. A comparação entre esses casos permitiu discutir potencialidades e limitações das diferentes abordagens, articulando a análise conceitual, os resultados empíricos recentes e o levantamento de políticas públicas em um quadro crítico sobre a construção da mensageria descentralizada como infraestrutura pública e bem comum digital.

3 INFRAESTRUTURA DIGITAL PÚBLICA E BENS COMUNS DIGITAIS

Infraestrutura digital pública (PDI) é entendida como um serviço de comunicação essencial gerido sob parâmetros públicos e não-extrativos[8]. Analogamente às ruas, redes elétricas ou protocolos básicos da internet, uma PDI maximiza valor público ao combinar atributos abertos (códigos, padrões e dados livres) com funções estatais ou coletivas. Na Web3, fala-se também em Digital Public Goods bens que são não-rivais, não-excludentes e desenvolvidos abertamente, geralmente sob licenças de código aberto[10]. Mensageria descentralizada encaixa-se nessa definição de duas formas:

In: I Workshop Brasileiro de Sistemas Web3 (BrWeb3 2025). Anais Estendidos do XXXI Simpósio Brasileiro de Sistemas Multimídia e Web (BrWeb3'2025). Rio de Janeiro/RJ, Brasil. Porto Alegre: Brazilian Computer Society, 2025.

ISSN 2596-1683

Como um serviço de comunicação fundamental para espaços públicos digitais, e também pode ser construído como software opensource e protocolo aberto, operado por comunidades. Ou seja, pode tornar-se uma infraestrutura pública digital ou bem comum digital.

Como ressalta Rozas[10], recursos mantidos por grandes comunidades colaborativas como software livre, enciclopédias online e plataformas de código aberto, exemplificam commons digitais globais. Estes sistemas coexistem sem hierarquia centralizada sendo sustentados por regras transparentes e participação comunitária. Protocolos de mensageria descentralizada (e.g. o protocolo Matrix ou plataformas baseadas em IPFS) seguem modelo semelhante: são especificações públicas, suportadas por comunidades de desenvolvedores e adotadas em ambientes públicos, e, portanto podem ser vistos como infraestruturas compartilhadas. De fato, projetos como o Matrix.org Foundation definem o protocolo Matrix como um common digital, ressaltando sua especificação aberta e governança coletiva[5]. Tais iniciativas ilustram que a comunicação criptografada e federada já está sendo pensada como infraestrutura comum na Web atual.

3.1 Abordagens de Mensageria Descentralizada

A seguir, resumimos os principais modelos de mensageria descentralizada identificados na literatura recente[15], apontando seus benefícios e limitações:

Esses três modelos representam trade-offs entre escalabilidade, privacidade e descentralização. Por exemplo, redes P2P evitam a dependência de um provedor único, mas exigem soluções próprias de sincronização; federação é mais madura tecnologicamente, porém carrega a questão da confiança nos donos de servidor; e abordagens blockchains concedem maior autogestão da identidade, porém não resolvem todos os desafios de performance. Novas propostas combinam elementos dessas abordagens para mitigar pontos fracos, reforçando aspectos como redundância de nós, criptografia ponta-a-ponta robusta e incentivos econômicos para participação.

3.2 Benefícios da Mensageria Descentralizada como Infraestrutura Pública

Tratar a mensageria descentralizada como infraestrutura pública digital traz vantagens sociais e técnicas. Segundo Frischmann[7] citado por fontes relevantes[8], infraestruturas são "meios compartilhados para muitos fins" que sustentam benefícios além dos interesses privados. Assim, investir em comunicações abertas gera externalidades positivas: inclusão digital, resistência à censura governamental ou comercial, e ambiente propício à inovação. Em especial, destacam-se:

- Controle de Dados pelo Usuário: Em infraestruturas descentralizadas, o usuário detém suas chaves e dados. Isso preserva a soberania digital individual, em linha com o conceito de propriedade comum. O fato de as mensagens não dependerem de um servidor único evita que a paralisação de uma empresa silencie comunidades inteiras.
- Resiliência e Confiabilidade: Redes federadas ou P2P naturalmente evitam pontos únicos de falha. Se um nó sai do ar, a rede continua funcionando. Para o público, isso significa maior disponibilidade do serviço de mensagens (característica essencial de uma infraestrutura pública).
- Inovação e Diversidade: Protocolos abertos e softwares livres facilitam criar novos clientes e servidores. Governos, ONGs e empresas podem customizar e integrar esses serviços sem pagar licenças, estimulando ecossistemas locais e soluções especializadas (e.g. aplicativos comunitários baseados em Matrix).
- Transparência e Governança Colaborativa: Modelos de commons digitais exigem regras claras para governança compartilhada. Projetos como Matrix.org e seu código aberto exemplificam isso: qualquer interessado pode participar do desenvolvimento, e a governança envolve uma comunidade técnica diversa. Essa transparência reforça a confiança pública, característica importante de serviço de bem comum.

4 DEPENDÊNCIA DE PLATAFORMAS CENTRALIZADAS ESTRANGEIRAS

A utilização generalizada de aplicativos de mensagens controlados por empresas estrangeiras (e.g. WhatsApp, Telegram, Signal...) pode minar a soberania nacional. Dados sensíveis transitam por servidores fora do controle estatal, sujeitos a leis externas como o USA PATRIOT Act e mecanismos de vigilância extraterritorial[11].

Pesquisas recentes ilustram de forma contundente os riscos de depender de plataformas centralizadas para comunicação política e social. Pinto e Silva [9] analisaram 67 grupos políticos no Telegram durante as eleições de 2022 e identificaram mais de 12 mil mensagens, com predominância de grupos de direita (50,9%) e picos de atividade nos turnos eleitorais. Já Venâncio et al. [14] mostraram como, em janeiro de 2023, cerca de 270 grupos e meio milhão de mensagens no Telegram serviram de base para a coordenação de atos antidemocráticos em Brasília. Esses estudos revelam que, embora populares, tais plataformas permitem tanto a concentração de fluxos informacionais quanto sua captura por grupos organizados, sem qualquer mecanismo público de auditoria ou governança.

Enquanto isso, o governo francês observou que as soluções comerciais "mantêm dados fora de nossos servidores" e estão potencialmente sujeitas a backdoors estrangeiros. Autoridades também apontam que plataformas centralizadas carecem de recursos de auditoria e fiscalização internos; por isso legisladores americanos pediram ao Departamento de Defesa que investigue protocolos descentralizados como alternativa mais segura[12], "não controlada por única empresa" e já usada por aliados da OTAN[6]. Essa fragilidade tem levado setores de defesa a rejeitar mensageiros comerciais: o Exército Brasileiro, por exemplo, proibiu oficiais de alta patente de usarem apps estrangeiros e criou o EBChat próprio, enquanto o Bundeswehr alemão abandonou serviços de consumo por considerá-los "completamente inadequados"[3] ao exigirem comunicação militar segura. Em suma, a dependência de sistemas proprietários estrangeiros expõe os países a riscos de vigilância externa, perda de controle de dados e fragilidade em momentos críticos.

5 INICIATIVAS GOVERNAMENTAIS DE MENSAGERIA DESCENTRALIZADA

Em reação a esses riscos, vários governos têm adotado ou incentivado soluções de mensageria baseadas em protocolos abertos e descentralizados. Na Europa, França e Alemanha lançaram apps

Table 1: Comparação de Modelos de Comunicação Descentralizada

Modelo	Características Principais	Vantagens	Desvantagens
Peer-to-Peer (P2P)	• Cada usuário é nó da rede • Sem servidor central • Exemplos: IRC, XMTP[2] • Identidade: Wallets blockchain (XMTP) • Armazenamento local	• Maior autonomia do usuário • Controle total da identidade	• Dificuldades de escalabilidade • Implantação complexa de criptografia E2E • Limitação em larga escala
Federação	• Múltiplos servidores interconectados • Qualquer entidade pode operar servidor • Exemplos: Matrix, XMPP • Identidade controlada pelo servidor • Armazenamento no servidor	• Alta disponibilidade (sem ponto único de falha) • Rede colaborativa	• Privacidade não garantida (admins acessam dados) • Regras variáveis por servidor • Risco de censura/leitura de conteúdos
Blockchain	• Blockchain como camada de identidade • Endereços de carteira como IDs • Exemplos: Mensageiros descentralizados • Identidade: Soberania do usuário • Armazenamento on-chain	• Soberania sobre identidade digital • Mensagens assinadas/verificadas • Integridade garantida	• Latência alta • Imutabilidade indesejada • Armazenamento inadequado para grandes volumes • Baixo desempenho

nacionais baseados no protocolo Matrix. Em 2018 a França desenvolveu o Tchap, sistema de mensagens próprio (cliente Riot/Element) para agentes públicos, argumentando que apps estrangeiros não garantiam "propriedade e soberania digital"[4] dos dados. O Tchap armazena dados em servidores governamentais e criptografia P2P, reforçando o controle estatal da informação. Na Alemanha, o BwMessenger (lançado em 2020) substituiu WhatsApp nas Forças Armadas; segundo fontes oficiais, o Matrix oferece "a soberania digital necessária" para comunicações em tempo real e uma rede aberta descentralizada, enquanto serviços comerciais foram considerados impróprios para uso militar.

Esse debate também começa a emergir no contexto brasileiro. Em agosto de 2025, a Agência Brasileira de Inteligência (ABIN) iniciou testes de uma plataforma própria de mensagens, apelidada de "WhatsApp estatal", destinada à comunicação interna do governo[1]. Tal iniciativa reflete a crescente preocupação com a soberania digital e a necessidade de reduzir a dependência de serviços estrangeiros para fluxos comunicacionais estratégicos, ainda que permaneça a questão sobre como garantir auditabilidade, interoperabilidade e governança pública em soluções nacionais.

Além da dimensão geopolítica, fatores psicológicos também influenciam a dinâmica de grupos em plataformas centralizadas. Vasconcelos et al. [13] demonstraram que a *curiosidade social* é um motor relevante na disseminação de mensagens em grupos políticos do Telegram. Mensagens apelativas relacionadas a urnas eletrônicas, religião ou intervenção militar obtiveram maior circulação justamente por explorarem variáveis como novidade, incerteza e conflito. Tais resultados ressaltam que, em ambientes sem governança aberta, a exploração de vieses cognitivos pode intensificar a desinformação. Nesse sentido, iniciativas como o Matrix, ao priorizarem transparência e auditabilidade, oferecem meios de mitigar essas dinâmicas de manipulação.

6 DESAFIOS E PERSPECTIVAS

Embora promissora, a transição para a mensageria descentralizada enfrenta desafios práticos. Entre eles estão a necessidade de redes robustas, a compatibilidade entre diferentes protocolos e o estabelecimento de padrões mínimos de segurança. Além disso, há uma dimensão regulatória e de financiamento: infraestrutura pública requer modelo de governança sustentável. Por exemplo, iniciativas

Table 2: Iniciativas Governamentais de Mensageria Segura

País/Organização	Projeto (Base)	Características e Justificativas
França	Tchap (Matrix)	• Mensageiro interno do governo • Substitui soluções convencionais que mantêm dados sob leis estrangeiras • Matrix garante soberania digital e auditoria
Alemanha	BwMessenger (Matrix)	• Aplicativo do exército alemão • Self-hosted, código aberto, criptografado • Proporciona "soberania digital necessária"
NATO/EUA	NI2CE (Matrix)	• Mensageiro federado para comunicações entre aliados • Usado por países-membros em defesa • Open-source, sem vendor lock-in • Pleito de expansão no Depto. de Defesa (EUA)
Brasil	EBChat (Signal) UNA Dígitro	• *EBChat*: Servidores militares nacionais • *UNA Dígitro*: Plataforma nacional (2025) • Produto Estratégico de Defesa

públicas podem subsidiar a operação de nós comunitários ou apoiar projetos de comunicação descentralizada, como já ocorre em alguns governos europeus, que adotam Matrix em suas instituições.

Para avançar nesta direção, propõe-se:

(1) Políticas Públicas de Apoio: Reconhecimento da mensageria descentralizada como um serviço essencial. Leis ou políticas podem incentivar o uso de protocolos abertos em comunicações governamentais, da mesma forma que existem programas de adoção de software livre.
(2) Desenvolvimento de Ferramentas Open Source: Criação e manutenção de clientes, servidores e gateways descentralizados, de código aberto. Exemplos incluem o servidor Synapse (Matrix) e clientes baseados em blockchain, que já seguem esta linha.
(3) Educação e Comunidade: Treinamento de desenvolvedores e usuários sobre privacidade e governança digital. Comunidades locais podem organizar salas federadas para cidadãos, ampliando o acesso gratuito e seguro à comunicação.
(4) Padrões Interoperáveis: Estabelecimento de protocolos comuns (e.g. XMTP, Matrix, ActivityPub) que permitam a troca de mensagens entre redes distintas. A interoperabilidade é chave para que a mensageria não se torne outro silo isolado.

7 CONSIDERAÇÕES FINAIS

A crescente centralização das plataformas de mensageria digital levanta preocupações estruturais sobre privacidade, interoperabilidade e soberania dos dados. Neste artigo, argumentou-se que sistemas descentralizados, baseados em protocolos abertos e software livre, constituem alternativas viáveis para reconfigurar a comunicação digital como infraestrutura pública.

Ao explorar abordagens técnicas como redes peer-to-peer, federação e soluções com identidade blockchain, identificamos um espectro de possibilidades que conciliam autonomia do usuário, resiliência técnica e transparência. Estas características se alinham à definição de bens comuns digitais e ampliam o potencial de inovação distribuída, controle democrático e inclusão comunicacional.

Avançar na consolidação da mensageria descentralizada como bem público exige o fortalecimento de ecossistemas abertos, o incentivo à adoção de padrões interoperáveis e a formulação de políticas públicas que reconheçam a comunicação como serviço essencial. Neste contexto, garantir a pluralidade arquitetural das infraestruturas digitais é uma condição fundamental para a autonomia tecnológica e a resiliência institucional das sociedades conectadas.

Como desdobramento futuro a este trabalho, propõe-se a realização de uma análise técnica aprofundada dos protocolos apresentados (em especial Matrix, XMTP e outras soluções emergentes) por meio de benchmarking comparativo. Tal estudo permitirá avaliar desempenho, escalabilidade, segurança e governança em cenários reais, fornecendo evidências experimentais que complementem a discussão conceitual aqui desenvolvida e orientem decisões de adoção em políticas públicas ou iniciativas comunitárias.

8 NOTA ÉTICA

Ressaltamos que ferramentas de Large Language Models (LLMs) foram empregadas como suporte no processo de escrita e organização textual. Todo o conteúdo técnico, análises e conclusões foram elaborados e validados pelos autores.

REFERENCES

[1] [n. d.]. Abin testa 'WhatsApp estatal' para comunicação interna do governo — www1.folha.uol.com.br. www1.folha.uol.com.br/poder/2025/08/abin-testa-whatsapp-estatal-para-comunicacao-interna-do-governo.shtml. [Accessed 10-08-2025].
[2] [n. d.]. Build with XMTP — docs.xmtp.org. https://docs.xmtp.org/. [Accessed 20-07-2025].
[3] [n. d.]. Bundeswehr | BwMessenger | Matrix | Defence case study — element.io. https://element.io/case-studies/bundeswehr. [Accessed 08-08-2025].
[4] [n. d.]. French government launches in-house developed messaging service, Tchap — interoperable-europe.ec.europa.eu. https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-messaging-service-tchap. [Accessed 08-08-2025].

[5] [n. d.]. Matrix Specification — spec.matrix.org. https://spec.matrix.org/latest/. [Accessed 20-07-2025].

[6] [n. d.]. NI2CE Messenger &x2013; The Innovation Hub for Allied Command Transformation — innovationhub-act.org. https://innovationhub-act.org/ni2ce-messenger/. [Accessed 08-08-2025].

[7] Brett M. Frischmann. 2012. *Infrastructure: The Social Value of Shared Resources*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199895656.001.0001

[8] Zuzanna Warso Jan Krewer. 2024. Digital Commons as Providers of Public Digital Infrastructures – Open Future — openfuture.eu. https://openfuture.eu/publication/digital-commons-as-providers-of-public-digital-infrastructures/. [Accessed 20-07-2025].

[9] Johnny Pinto and Thiago Silva. 2023. Caracterização de Grupos Políticos no Telegram Durante a Eleição Presidencial de 2022. In *Anais Estendidos do XXIX Simpósio Brasileiro de Sistemas Multimídia e Web* (Ribeirão Preto/SP). SBC, Porto Alegre, RS, Brasil, 55–58. https://doi.org/10.5753/webmedia_estendido.2023.235697

[10] David Rozas, Antonio Tenorio-Fornés, and Samer Hassan. 2021. Analysis of the Potentials of Blockchain for the Governance of Global Digital Commons. *Frontiers in Blockchain* 4 (April 2021). https://doi.org/10.3389/fbloc.2021.577680

[11] Ericson Scorsim. [n. d.]. A política externa dos Estados Unidos e a soberania brasileira - Portal Direito da Comunicação — direitodacomunicacao.com. https://direitodacomunicacao.com/br/a-geoestrategica-dos-estados-unidos-e-sua-politica-externa-rule-of-law-hard-power-e-softpower-norte-americanos-e-a-influencia-sobre-o-brasil-a-necessaria-compreensao-do-tema-para-a-protecao-da-sobe/. [Accessed 05-08-2025].

[12] Ron Wyden (United States Senator). [n. d.]. wyden.senate.gov. https://www.wyden.senate.gov/imo/media/doc/wyden-schmitt_dod_letter.pdf. [Accessed 07-08-2025].

[13] Francisco Vasconcelos, Alexandre Sousa, and Jussara Almeida. 2024. A social curiosity-driven approach to analyzing the information dissemination in Telegram political groups. In *Anais Estendidos do XXX Simpósio Brasileiro de Sistemas Multimídia e Web* (Juiz de Fora/MG). SBC, Porto Alegre, RS, Brasil, 33–36. https://doi.org/10.5753/webmedia_estendido.2024.244422

[14] Otávio Venâncio, Gabriel Gonçalves, Carlos Ferreira, and Ana Silva. 2024. Evidências de disseminação de conteúdo no Telegram durante o ataque aos órgãos públicos brasileiros em 2023. In *Proceedings of the 30th Brazilian Symposium on Multimedia and the Web* (Juiz de Fora/MG). SBC, Porto Alegre, RS, Brasil, 385–389. https://doi.org/10.5753/webmedia.2024.241972

[15] Mason Yeung. 2024. SendingNetwork: Advancing the Future of Decentralized Messaging Networks. arXiv:2401.09102 [cs.SI] https://arxiv.org/abs/2401.09102