Uma Arquitetura Baseada em Blockchain para Comunicação entre Sistemas de Acesso ao Espectro

Alan Veloso[1], **Jeffson Sousa**[1,2], **Diego Abreu**[1], **Antônio Abelém**[1]

[1] Universidade Federal do Pará (UFPA)
Belém – PA – Brasil

[2]Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

aveloso@ufpa.br, jcsousa@cpqd.com.br
diego.abreu@itec.ufpa.br, abelem@ufpa.br

Abstract. *This paper proposes an architecture for Spectrum Access Systems (SAS) integrated with permissioned blockchain technology to enhance security, traceability, and interoperability in the communication among different SAS instances. The approach leverages smart contracts to automate data usage agreements, device registration, and spectrum coordination, replacing traditional REST interfaces with a distributed and auditable infrastructure. The proposed model is validated through a practical implementation using Hyperledger Besu, demonstrating feasibility and compliance with regulatory requirements. The hybrid solution offers advantages such as data immutability, shared governance, and operational resilience.*

Resumo. *Este artigo propõe uma arquitetura para Sistemas de Acesso ao Espectro (SAS) com integração à tecnologia blockchain permissionada, visando aumentar a segurança, rastreabilidade e interoperabilidade na comunicação entre diferentes instâncias de SAS. A abordagem utiliza contratos inteligentes para automatizar acordos de uso de dados, registro de dispositivos e coordenação de espectro, substituindo interfaces REST tradicionais por uma infraestrutura distribuída e auditável. A proposta é validada por meio de um módulo implementado com Hyperledger Besu, demonstrando viabilidade prática e compatibilidade com requisitos regulatórios. A solução híbrida oferece vantagens como imutabilidade dos dados, governança compartilhada e resiliência operacional.*

1. Introdução

O crescimento exponencial da demanda por conectividade e aplicações móveis de alto desempenho tem impulsionado a evolução das redes móveis rumo às tecnologias 5G e, futuramente, 6G [Salahdine et al. 2023]. Esses novos paradigmas de comunicação exigem um gerenciamento mais eficiente e dinâmico do espectro de radiofrequência, recurso escasso e essencial para a qualidade e confiabilidade dos serviços [Alsaedi et al. 2023]. Nesse cenário, torna-se fundamental o desenvolvimento de infraestruturas inteligentes de gerenciamento de espectro, capazes de atender às crescentes necessidades de mobilidade, baixa latência, alta densidade de dispositivos e reconfiguração em tempo real, características fundamentais das redes móveis de nova geração.

O *Spectrum Access System* (SAS) surge como solução regulatória e tecnológica para viabilizar o compartilhamento dinâmico do espectro, como no *Citizens Broadband Radio Service* (CBRS) dos Estados Unidos. Entretanto, a interface SAS–SAS baseada em REST sobre HTTPS já demonstra fragilidades em ambientes 5G/6G: (i) o *Threat Model* do WInnForum alerta que a violação de uma autoridade certificadora pode gerar certificados falsos e ataques Sybil [Wireless Innovation Forum 2016]; (ii) relatórios de testes no Google SAS Portal registram falhas recorrentes de handshake TLS entre implementações de fornecedores distintos [Google Cloud SAS Team 2025]; e (iii) o documento "*Lessons Learned from CBRS*" destaca a falta de trilhas de auditoria consolidadas, dificultando a responsabilização em tempo real [Wireless Innovation Forum 2022a]. Esses exemplos reforçam que o modelo atual carece de garantias robustas de segurança, transparência e coordenação — lacunas que uma infraestrutura blockchain permissionada pode suprir ao prover imutabilidade dos registros, autenticação forte distribuída e governança compartilhada.

Diante desse contexto, levanta-se a seguinte questão de pesquisa: *como garantir uma comunicação segura, auditável e interoperável entre Sistemas de Acesso ao Espectro (SAS), alinhada às exigências das redes móveis 5G/6G, sem comprometer desempenho e conformidade regulatória?*

A justificativa deste trabalho reside no potencial da tecnologia de blockchain permissionada, que oferece mecanismos nativos de autenticação forte, imutabilidade dos dados, rastreabilidade e automação por meio de contratos inteligentes. Essas propriedades podem atender diretamente aos requisitos funcionais da comunicação entre SASs, permitindo que a troca de informações entre sistemas seja mais confiável, auditável e resiliente. Tais características são especialmente importantes para o gerenciamento inteligente de redes móveis, em que diferentes operadores e entidades compartilham dinamicamente os recursos de espectro.

O objetivo principal deste artigo é propor uma arquitetura híbrida para Sistemas de Acesso ao Espectro com integração blockchain, na qual a comunicação entre SASs ocorre por meio de uma rede blockchain permissionada, sem substituir os mecanismos operacionais internos. A arquitetura busca garantir segurança, transparência, interoperabilidade e governança distribuída, aspectos essenciais para atender aos requisitos das redes móveis emergentes.

As principais contribuições deste trabalho incluem:

- A proposição de uma arquitetura baseada em blockchain para comunicação inter-SAS voltada a cenários de redes móveis 5G/6G;
- A análise da aderência da tecnologia blockchain aos requisitos funcionais da interface SAS-SAS;
- A descrição detalhada dos componentes, fluxos operacionais e aspectos de governança da arquitetura proposta;
- A apresentação de um exemplo prático de implementação com Hyperledger Besu;
- A discussão crítica sobre as vantagens, limitações e caminhos de evolução da proposta no contexto do gerenciamento de redes móveis.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta uma análise de um conjunto de trabalhos que se relacionam com a proposta; a Seção 3 apresenta os

fundamentos do SAS e suas interfaces principais; a Seção 4 detalha os requisitos funcionais da interface SAS-SAS; a Seção 5 discute como a tecnologia blockchain atende a esses requisitos; a Seção 6 apresenta a arquitetura proposta com integração blockchain; a Seção 7 descreve um exemplo de implementação prática; a Seção 8 discute vantagens e desafios da abordagem; e, por fim, a Seção 9 traz as considerações finais e trabalhos futuros.

2. Trabalhos Relacionados

Trabalhos recentes têm investigado o uso de tecnologias blockchain para apoiar o gerenciamento dinâmico do espectro, especialmente no contexto do *Spectrum Access System* (SAS) e do CBRS. Tais propostas têm como objetivo superar limitações de confiabilidade, escalabilidade e segurança inerentes ao modelo centralizado tradicional.

Em [Xiao et al. 2023], os autores propõem o BD-SAS, uma arquitetura descentralizada baseada em blockchain que introduz duas camadas: uma cadeia global (G-Chain), voltada para tarefas regulatórias e sincronização entre SASs, e cadeias locais (L-Chains), responsáveis pela alocação de espectro em regiões específicas. A arquitetura também inclui mecanismos de *reshuffling* de servidores SAS para tolerância a falhas e resistência a adversários adaptativos. Essa proposta se aproxima do modelo apresentado neste trabalho, especialmente no tocante à descentralização dos processos de decisão e sincronização entre SASs.

Li et al. [Li et al. 2023] apresentam um *framework* para compartilhamento dinâmico de espectro entre múltiplos operadores, suportado por uma blockchain de consórcio. A proposta inclui a utilização de contratos inteligentes e um modelo baseado em jogo Stackelberg para precificação ótima de espectro, destacando a flexibilidade dos operadores em atuarem como provedores ou requisitantes de espectro conforme sua demanda. Embora o foco seja voltado para o mercado inter-operador, as contribuições sobre governança descentralizada e incentivos são relevantes para SASs distribuídos.

Em [Wu et al. 2023], os autores introduzem o SpectrumChain, um *framework* para compartilhamento dinâmico de espectro visando redes 6G. A arquitetura propõe o uso de blockchain hierárquico para registrar alocação de espectro e assegurar a rastreabilidade das transações, integrando sensores cognitivos para suporte à decisão. Essa abordagem destaca-se pela ênfase na escalabilidade e nas aplicações emergentes de redes heterogêneas.

A proposta do B-CBRS, apresentada em [Li et al. 2021], utiliza blockchain para coordenar o acesso ao espectro por usuários *General Authorized Access*, delegando aos usuários *Priority Access* a responsabilidade de gerenciar as alocações com base em contratos inteligentes e algoritmos de alocação ótimos. Esse modelo reforça a viabilidade de estruturas descentralizadas mesmo sob a hierarquia tradicional de acesso ao espectro.

Além dessas propostas específicas, levantamentos abrangentes também têm sido conduzidos. O trabalho de Perera et al. [Perera et al. 2024] apresenta um *survey* detalhado sobre o uso de blockchain para o gerenciamento dinâmico de espectro. O artigo destaca os benefícios, desafios e oportunidades da aplicação de blockchain no contexto de acesso dinâmico ao espectro, classificando as soluções existentes quanto ao tipo de arquitetura, comportamento de sensoriamento e métodos de acesso. Além disso, aponta lacunas de

pesquisa e discute direções futuras, posicionando-se como uma referência importante para fundamentar novas arquiteturas, como a proposta neste trabalho.

A presente proposta diferencia-se por aplicar os conceitos de blockchain permissionada ao contexto da interface SAS-SAS, promovendo sincronização auditável e segura entre instâncias SAS e explorando os recursos nativos de imutabilidade, controle de acesso e execução automatizada via contratos inteligentes.

Como evidencia a Tabela 1, apenas a proposta aqui apresentada combina simultaneamente quatro atributos cruciais — segurança, interoperabilidade, rastreabilidade e uso de blockchain permissionada — focados diretamente na interface SAS–SAS. Enquanto trabalhos anteriores tratam esses requisitos de forma parcial (por exemplo, BD-SAS privilegia escalabilidade, mas não aborda interoperabilidade em profundidade, e as soluções voltadas à interface SAS–CBSD concentram-se em mecanismos de incentivo econômico), o nosso modelo oferece uma abordagem que abrange tanto a proteção criptográfica dos registros quanto a padronização do esquema de dados e a auditabilidade completa das operações entre diferentes provedores de SAS. Essa cobertura multidimensional reforça o potencial da arquitetura proposta para servir como referência de base para futuras atualizações do padrão SAS.

Tabela 1. Comparação entre propostas que aplicam blockchain ao gerenciamento dinâmico de espectro.

Trabalho	Tipo	Interf.	Seg.	Interop.	Rast.	Escalab.	Incent.
BD-SAS	Pública	SAS–SAS	✓	—	✓	✓	—
SpectrumChain	Pública	SAS–SAS	✓	—	✓	✓	—
B-CBRS	Pública	SAS–CBSD	—	—	✓	—	✓
Multi-operator	Perm.	SAS–CBSD	—	✓	—	—	✓
Nossa proposta	Perm.	SAS–SAS	✓	✓	✓	—	—

3. Sistema de Acesso ao Espectro (SAS)

O SAS é uma plataforma centralizada de gerenciamento dinâmico de espectro desenvolvida para viabilizar o uso eficiente da faixa de 3550–3700 MHz, no contexto do CBRS nos Estados Unidos. Este sistema é responsável por coordenar o acesso ao espectro entre diferentes camadas de usuários — incluindo usuários incumbentes federais, titulares de *Priority Access License* (PAL) e usuários de *General Authorized Access* (GAA) — garantindo proteção contra interferência e conformidade com as normas regulatórias da *Federal Communications Commission* (FCC) [Wireless Innovation Forum 2020, Wireless Innovation Forum 2022b].

O SAS desempenha funções críticas, tais como:

- Autorização de uso do espectro para dispositivos de redes do CBRS;
- Proteção a usuários incumbentes (ex.: radares navais);
- Gerenciamento de zonas de proteção (ex.: áreas PAL);
- Coordenação de eventos regulatórios e mitigação de interferências.

Para viabilizar essas funcionalidades, o SAS se comunica com os dispositivos de rede CBRS, denominados *Citizens Broadband Radio Service Devices* (CBSDs), e outros SASs por meio de duas interfaces principais padronizadas: Interface SAS-CBSD e Interface SAS-SAS. Descritas a seguir.

3.1. Interface SAS-CBSD

A interface SAS-CBSD (Figura 1) define o protocolo de comunicação entre o SAS e os dispositivos finais que operam na banda CBRS, os CBSDs. Essa interface especifica procedimentos como:

- Registro do CBSD;
- Consulta de espectro disponível;
- Solicitação e concessão de autorizações de transmissão;
- Batimentos periódicos para manutenção da autorização (*Heartbeat*);
- Renúncia e desregistro de dispositivos.

As mensagens são codificadas em JSON e transportadas via HTTPS com autenticação mútua baseada em certificados X.509.

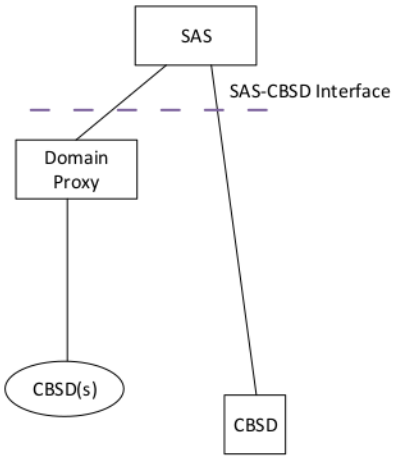

Figura 1. Interface SAS-CSBD [Wireless Innovation Forum 2022b].

3.2. Interface SAS-SAS

A interface SAS-SAS trata da comunicação entre diferentes implementações do SAS, permitindo a troca de informações para assegurar a consistência e a interoperabilidade do sistema como um todo. Essa interface viabiliza:

- Sincronização de registros de CBSDs, zonas geográficas e eventos de coordenação;
- Compartilhamento de dados de sensores ESC (*Environmental Sensing Capability*);
- Coordenação de zonas de proteção e ações regulatórias;
- Suporte a mecanismos de *Push* e *Pull* para transferência de registros.

A interface SAS-SAS também utiliza protocolos seguros com TLS v1.2 e autenticação mútua, garantindo a integridade e a confidencialidade dos dados trocados entre instâncias do SAS.

4. Requisitos Funcionais do SAS-SAS Interface

Esta seção descreve os requisitos funcionais necessários para a implementação da interface de comunicação entre sistemas de gerenciamento de espectro automatizados. Os requisitos visam garantir segurança, interoperabilidade e consistência na troca de informações entre SASs pares.

- **Autenticação e Segurança:** A comunicação entre SASs deve ser protegida por autenticação mútua baseada em TLS v1.2[1], com verificação de certificados digitais. A negociação de *ciphersuites* seguras é obrigatória para assegurar a confidencialidade e integridade dos dados transmitidos. Conexões devem ser terminadas imediatamente em caso de falhas na autenticação.
- **Descoberta de SASs Pares:** O sistema deve suportar mecanismos de descoberta estática e dinâmica de SASs pares, por meio de serviços como DNS ou DHCP. Além disso, deve ser possível registrar e manter os *endpoints* de comunicação com os SASs descobertos.
- **Acordo de Uso de Dados:** Deve-se estabelecer acordos explícitos sobre as restrições de uso dos dados compartilhados com SASs pares, visando garantir conformidade com normas regulatórias e políticas de privacidade.
- **Troca de Registros:** A interface deve possibilitar a troca estruturada de registros referentes a: Dispositivos CBSD; Zonas protegidas (PAL, PPA, zonas de exclusão, entre outras); Eventos de Coordenação; Sensores ESC; Implementações SAS e informações sobre administradores SAS. Cada registro deve possuir um identificador único, com hierarquia baseada em *namespace*.
- **Sincronização de Dados:** A interface deve suportar solicitações por intervalo de tempo (*time-range requests*) para CBSDs, zonas e eventos de coordenação. Cada solicitação pode cobrir no máximo 25 horas de dados, os quais devem permanecer disponíveis por um período mínimo de 30 dias. As respostas devem conter apenas registros modificados no intervalo especificado, aplicando filtros específicos, como a seleção de CBSDs com *grants* ativos ou pendentes.
- **Solicitações por Identificador:** Deve-se permitir a recuperação de informações detalhadas de registros específicos com base em seus identificadores únicos (requisições *by-ID*).
- **Troca de Dados via *Push*:** A interface deve ser capaz de processar requisições do tipo *Push*, contendo dados atualizados sobre CBSDs, zonas e eventos de coordenação. O sistema deve responder utilizando códigos HTTP apropriados (ex.: 200, 422, 50x).
- **Geração de *Dumps* Completos:** O SAS deve gerar periodicamente, no mínimo a cada sete dias, um *Full Record Dump* contendo: CBSDs com *grants* ativos ou pendentes; Zonas protegidas (PAL, PPA ou ad hoc); Sensores ESC afiliados. Esses arquivos devem permanecer disponíveis por pelo menos 14 dias para acesso pelos SASs pares.
- **Fluxos de Mensagens:** A interface deve suportar tanto fluxos do tipo *Pull* (sob demanda) quanto *Push* (proativos). Deve-se garantir a resiliência e continuidade das comunicações mesmo em cenários de falha parcial da rede.

5. Aderência da Tecnologia Blockchain aos Requisitos Funcionais

A tecnologia blockchain apresenta características que podem contribuir significativamente para o atendimento dos requisitos funcionais descritos para sistemas de troca segura e auditável de dados entre SASs. A seguir, descrevemos como as funcionalidades inerentes a

[1]A versão foi escolhida por compatibilidade: a especificação oficial da interface SAS–SAS (WINNF-TS-0096) ainda referencia TLS v1.2, e o acarbouço de teste público da Wireless Innovation Forum (`https://github.com/Wireless-Innovation-Forum/Spectrum-Access-System`) foi desenvolvido considerando essa versão.

Tabela 2. Correspondência entre requisitos funcionais da interface SAS–SAS e as características oferecidas por uma blockchain permissionada.

Requisito funcional	**Características da blockchain que o satisfazem**
Autenticação e segurança	Certificados X.509 para nós validadores; TLS v1.2 com pinagem de chave; transações assinadas; consenso IBFT 2.0 garante integridade de blocos.
Descoberta de SASs pares	*Endpoints* publicados como transações imutáveis; *events* de contrato notificam a chegada de novos pares.
Acordo de uso de dados	Cláusulas codificadas em contratos inteligentes; execução automática auditável e não-repúdio.
Troca de registros (CBSD, zonas, eventos)	*Ledger* distribuído armazena todos os registros; replicação garante disponibilidade e consistência global.
Sincronização de dados por intervalo	Carimbos de tempo e altura de bloco; consultas por janela temporal retornam somente mudanças.
Solicitações por identificador	Funções `view` devolvem o registro exato via `getById(hash)`.
Troca de dados via *push*	Publicação de transações/eventos; assinantes Web3 reagem em tempo (quase) real.
Geração de *dumps* completos	Histórico integro no *ledger*; *queries* programáticas produzem *dumps* periódicos ($\geq$ 14 dias).
Fluxos *pull*/*push* resilientes	Replicação bizantina (IBFT 2.0); tolerância a falhas de nós e re-execução determinística de blocos.

blockchains podem ser aplicadas em cada um dos requisitos elencados e a Tabela 2 traz um resumo.

A infraestrutura de blockchain permissionada, como Hyperledger Fabric ou Besu, permite autenticação mútua baseada em certificados digitais (e.g., X.509), integrada à negociação de canais seguros via TLS v1.2. A verificação criptográfica das transações e blocos garante integridade e confidencialidade, enquanto políticas de controle de acesso podem ser aplicadas nos canais de comunicação para restringir o acesso apenas a entidades autorizadas. O suporte nativo à revogação de certificados e monitoramento de eventos permite o encerramento de conexões TLS em casos de falhas na autenticação.

Embora a descoberta dinâmica de peers (via DNS/DHCP) seja tradicionalmente realizada fora do escopo do blockchain, os dados de registro de *endpoints* e associações entre SASs podem ser armazenados e compartilhados de forma imutável na própria rede blockchain. A sincronização desses registros garante rastreabilidade e confiabilidade na descoberta e manutenção das conexões com pares.

Contratos inteligentes permitem a definição e aplicação automática de acordos de uso de dados entre SASs. As cláusulas contratuais podem ser registradas de forma imutável, e sua execução automatizada garante conformidade com os termos acordados, possibilitando auditoria transparente e não repudiável.

A blockchain pode ser utilizada como repositório confiável para a troca de infor-

mações sobre CBSDs, zonas regulatórias (PAL, PPA, exclusão), sensores ESC e eventos de coordenação. O uso de identificadores únicos com estrutura hierárquica (e.g., com *namespace*) pode ser incorporado diretamente nos registros armazenados em blocos, facilitando a indexação e recuperação eficiente de dados.

A rastreabilidade inerente ao blockchain permite a realização de requisições por intervalo de tempo, visto que cada transação e bloco possuem registros temporais (*timestamps*). Dessa forma, é possível consultar registros modificados em janelas específicas, garantindo integridade histórica. Além disso, dados mantidos na blockchain atendem naturalmente à exigência de retenção mínima (e.g., 30 dias), com possibilidade de aplicar filtros via contratos inteligentes.

A recuperação de dados específicos por identificador único pode ser realizada por meio de funções de consulta nos contratos inteligentes, garantindo acesso a registros detalhados e imutáveis conforme o ID consultado, respeitando a estrutura definida de nomes hierárquicos.

Eventos proativos (*Push*) podem ser modelados na blockchain por meio de transações submetidas diretamente por pares autorizados. A confirmação de inclusão em bloco, bem como a verificação dos códigos de resposta (e.g., 200 OK, 422 *Unprocessable Entity*), pode ser associada a eventos nos contratos inteligentes, promovendo comunicação robusta e verificável.

A geração de *dumps* periódicos pode ser automatizada com base na consulta da blockchain por critérios predefinidos (e.g., CBSDs ativos, zonas protegidas, sensores ESC). Tais *dumps* podem ser armazenados em repositórios descentralizados ou extraídos diretamente via APIs de leitura, garantindo disponibilidade por períodos superiores a 14 dias conforme exigido.

Embora a blockchain não defina o transporte de mensagens em si, interfaces RESTful sobre HTTPS/TLS podem ser utilizadas para enviar/receber dados em formato JSON (RFC-7159), garantindo compatibilidade com os protocolos estabelecidos para codificação e transporte de mensagens.

A blockchain suporta tanto fluxos *Pull* (via consultas a registros) quanto *Push* (via inserção de novas transações), oferecendo resiliência por meio de replicação distribuída dos dados. Isso assegura continuidade da operação mesmo diante de falhas em nós individuais ou interrupções temporárias de comunicação.

Dessa forma, observa-se que a adoção de tecnologias blockchain pode aumentar a confiança, rastreabilidade e automação na comunicação entre SASs, alinhando-se a requisitos regulatórios e operacionais de ambientes cooperativos e altamente sensíveis à integridade dos dados.

6. Arquitetura Proposta com Integração Blockchain

A Figura 2 apresenta uma visão sistêmica da arquitetura proposta para SAS com integração de blockchain permissionada. Nesta abordagem, a blockchain é utilizada como infraestrutura de confiança para troca segura e auditável de informações entre SASs, sem substituir completamente os componentes operacionais internos.

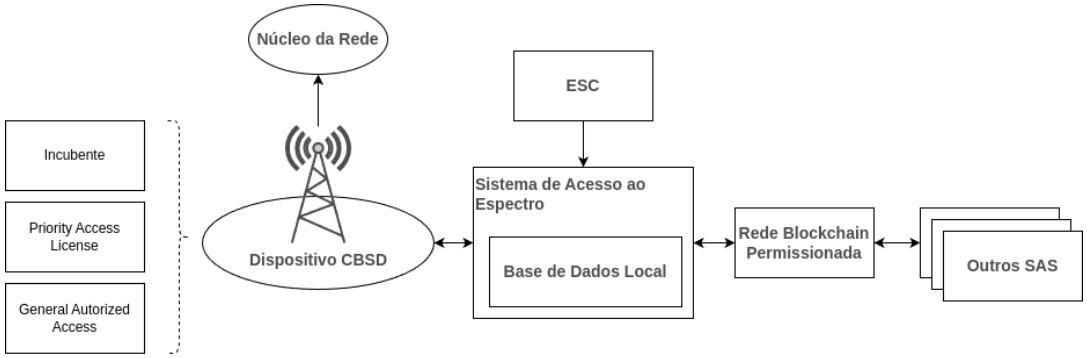

Figura 2. Arquitetura SAS com integração à Rede Blockchain Permissionada

6.1. Componentes Arquiteturais

A arquitetura é composta pelos seguintes elementos principais:

- **Dispositivo CBSD (*Citizen Broadband Radio Service Device*):** Equipamento responsável pela operação no espectro dinâmico. Envia informações sobre localização, potência e demandas de espectro ao SAS. Incluem *Incumbentes*, PAL e GAA, que representam diferentes níveis de prioridade no acesso ao espectro, conforme definido pelas regras de compartilhamento.
- **Sistema de Acesso ao Espectro:** Responsável pela coordenação de uso do espectro, concessão de *grants* e comunicação com CBSDs e outros SASs. Internamente, o SAS mantém uma Base de Dados Local, utilizada para decisões rápidas e armazenamento temporário.
- **ESC (*Environmental Sensing Capability*):** Sistema de sensores dedicado à detecção de sinais de incumbentes. O SAS pode utilizar os dados do ESC para evitar interferências prejudiciais.
- **Rede Blockchain Permissionada:** Funciona como meio de comunicação oficial entre SASs. Informações relevantes como registros de CBSDs, zonas protegidas, *grants*, eventos de coordenação e acordos de uso são publicados nesta rede, garantindo rastreabilidade, segurança e transparência.
- **Outros SASs:** Representam as instâncias externas com as quais o SAS local precisa se comunicar. Toda interação ocorre exclusivamente por meio da rede blockchain permissionada.

6.2. Fluxo Operacional

O funcionamento da arquitetura proposta segue os seguintes passos principais:

1. O CBSD envia suas informações operacionais ao SAS local.
2. O SAS consulta sua base de dados local para verificar disponibilidade de espectro e políticas internas.
3. Caso necessário, o SAS publica ou consulta informações na blockchain para verificar *grants* ativos, eventos de coordenação e dados de CBSDs vizinhos.
4. O SAS interage com outros SASs exclusivamente por meio da blockchain permissionada, utilizando contratos inteligentes para registrar atualizações, consultar informações por ID ou intervalo temporal, e validar acordos de dados.
5. *Dumps* periódicos e notificações *push* são emitidos como transações na blockchain, assegurando visibilidade compartilhada e integridade.

6. Dados de sensores ESC são considerados localmente e podem ser compartilhados, se necessário, via blockchain.

6.3. Vantagens do Modelo Híbrido com Blockchain

Este modelo preserva a arquitetura clássica de um SAS com base local de operação e gerenciamento de espectro, enquanto adiciona uma camada robusta de comunicação inter-SAS por meio da blockchain. Dentre os benefícios, destacam-se:

- Transparência e rastreabilidade entre operadores SAS.
- Eliminação de canais REST externos entre SASs, reduzindo vetores de ataque.
- Imutabilidade e auditoria nativa de todos os registros e trocas de mensagens.
- Execução automatizada de acordos e políticas via contratos inteligentes.

A governança da rede blockchain permissionada é compartilhada entre os operadores SAS, que atuam como nós validadores. A interoperabilidade é assegurada por contratos inteligentes padronizados e esquemas de dados comuns, permitindo que diferentes SASs interajam de forma transparente e segura.

7. Exemplo: Módulo em Solução Descentralizada de Compartilhamento de Infraestrutura de Redes Baseada em Blockchain

Essa proposta foi implementada como um módulo em uma solução descentralizada de compartilhamento de infraestrutura de redes baseada em blockchain [Sousa et al. 2024]. Este projeto é uma parceria entre a Universidade Federal do Pará (UFPA) e Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD).

Para demonstrar a aplicabilidade da arquitetura proposta, apresenta-se um exemplo prático de implementação baseado na integração de um SAS com uma Tecnologia de Registro Distribuído (*Distributed Ledger Technology* - DLT) permissionada Hyperledger Besu[2]. O Hyperledger Besu possui algumas políticas de acesso diferentes das de uma blockchain "tradicional" (pública em sua essência) [Scheid et al. 2021].

A proposta considera uma rede de SASs coordenada por contratos inteligentes, na qual toda comunicação entre sistemas ocorre de maneira distribuída, segura e auditável, utilizando a blockchain como meio oficial de interação. O conjunto de tecnologias utilizadas nessa implementação pode ser visto na Tabela 3

Tabela 3. Tecnologias utilizadas na implementação exemplo

Componente	**Tecnologia Utilizada**
Plataforma Blockchain	Besu (IBFT 2.0)
Contratos Inteligentes	Solidity + Hardhat Framework
Gerenciamento de Identidades	Certificados X.509 com TLS v1.2
Persistência Local do SAS	PostgreSQL
Serviço de Aplicação SAS	Node.js + Express.js (REST interno)
Monitoramento e Auditoria	Prometheus + Grafana
Interface de Consulta Blockchain	Web3.js + APIs REST locais

[2]O código-fonte relacionado à implementação apresentada ainda não pode ser disponibilizado publicamente devido a restrições de privacidade e confidencialidade do projeto.

Neste cenário, cada SAS opera localmente com sua própria base de dados, responsável pelo gerenciamento de dispositivos CBSD, análise de zonas, monitoramento de sensores ESC e tomada de decisão quanto à concessão de *grants*. No entanto, ao invés de utilizar canais diretos como REST ou outras interfaces tradicionais para compartilhar informações com SASs pares, todos os dados relevantes — incluindo registros de CBSDs, atualizações de zonas protegidas, notificações de coordenação e acordos de uso de dados — são registrados como transações na blockchain permissionada baseada no Besu[3].

A infraestrutura da rede blockchain utiliza o mecanismo de consenso IBFT 2.0, adequado para ambientes permissionados que exigem finalização rápida das transações e tolerância a falhas bizantinas. Cada operador SAS participa da rede como um nó validador, sendo identificado por certificados digitais X.509, assegurando autenticação robusta e controle de acesso distribuído. As funções operacionais são modeladas em contratos inteligentes escritos em Solidity, os quais são responsáveis por estruturar as operações de leitura e escrita na blockchain.

O sistema SAS é implementado com tecnologias amplamente utilizadas no desenvolvimento de sistemas distribuídos. A lógica de aplicação e os serviços locais são desenvolvidos em Node.js, utilizando o *framework* Express.js[4], enquanto os dados locais são persistidos em PostgreSQL[5]. As interações com a blockchain são realizadas via biblioteca Web3.js[6], tanto para submissão de transações quanto para escuta de eventos emitidos pelos contratos inteligentes. Assim, ações como a publicação de registros de CBSD, a emissão de *dumps* periódicos ou a resposta a solicitações por ID são acionadas diretamente no ambiente blockchain.

Para garantir a visibilidade e auditoria contínua, a arquitetura incorpora ferramentas de monitoramento e análise baseadas em Prometheus[7] e Grafana[8]. Esses sistemas permitem acompanhar métricas de uso da blockchain, como volume de transações, tempo médio de propagação dos blocos, frequência de atualizações entre SASs e latência média entre eventos registrados.

A adoção do Besu nessa arquitetura possibilita uma série de benefícios. Primeiramente, sua compatibilidade com a *Ethereum Virtual Machine* (EVM) oferece flexibilidade no desenvolvimento e reuso de contratos inteligentes. Além disso, a utilização de APIs JSON-RPC padronizadas facilita a integração com sistemas legados e ferramentas de monitoramento. Por fim, o suporte a mecanismos de privacidade como Tessera[9] pode ser incorporado em versões futuras, caso haja necessidade de manter registros confidenciais entre subconjuntos de participantes da rede.

Este exemplo evidencia que, ao integrar blockchain como infraestrutura nativa de comunicação entre SASs, é possível atender aos requisitos regulatórios de segurança, rastreabilidade e integridade, ao mesmo tempo em que se constrói uma base tecnológica escalável e interoperável para gestão dinâmica do espectro.

---

[3] https://besu.hyperledger.org/
[4] https://expressjs.com/pt-br/
[5] https://www.postgresql.org/
[6] http://web3js.org/
[7] https://prometheus.io/
[8] https://grafana.com/
[9] https://docs.tessera.consensys.io/

8. Discussão

A aplicação da tecnologia blockchain no contexto de comunicação entre SASs oferece diversos benefícios, especialmente no que tange à segurança, rastreabilidade e governança descentralizada. No entanto, também impõe desafios técnicos e operacionais que devem ser considerados. Esta seção discute as principais vantagens e desvantagens da adoção de blockchain frente aos requisitos funcionais descritos.

A principal contribuição da blockchain reside na imutabilidade dos dados registrados, garantindo que todas as trocas de informações, acordos e atualizações possam ser auditadas de forma confiável, com trilhas de auditoria que fortalecem a conformidade regulatória. Os mecanismos nativos de autenticação, como certificados digitais, assinaturas criptográficas e canais TLS, reforçam a segurança das comunicações, enquanto a natureza distribuída da rede reduz pontos únicos de falha.

Além disso, a possibilidade de codificar políticas de uso, regras de acesso, filtros e notificações diretamente em contratos inteligentes oferece automação confiável e elimina ambiguidades nos acordos operacionais entre SASs pares. Como os dados são replicados entre os nós participantes, falhas em um ou mais nós não comprometem a continuidade das operações, favorecendo sistemas críticos como os de gestão de espectro. Em redes permissionadas, também é possível garantir visibilidade seletiva de dados, equilibrando transparência operacional com privacidade institucional e conformidade regulatória.

A replicação dos dados em todos os nós da rede pode resultar em maior uso de recursos computacionais e de armazenamento, especialmente quando há necessidade de retenção de registros históricos por longos períodos. Além disso, a confirmação de transações e a propagação de blocos podem introduzir latências relevantes, o que se torna crítico em casos que exigem atualização em tempo quase real, como notificações de coordenação espectral.

A introdução de uma camada de blockchain também implica mudanças na arquitetura dos sistemas legados, exigindo capacitação das equipes para o desenvolvimento e manutenção de contratos inteligentes e nós validadores. Outro desafio está na definição de políticas de consenso, identidade e permissão entre diferentes operadores SAS, especialmente em cenários com múltiplas jurisdições ou interesses institucionais distintos.

Embora blockchains permissionadas ofereçam melhor desempenho em comparação às públicas, ainda podem enfrentar limitações de escalabilidade em ambientes com grandes volumes de dados e transações simultâneas.

A escolha pela adoção de blockchain deve considerar o equilíbrio entre os benefícios de segurança, transparência e rastreabilidade, e os custos operacionais e técnicos associados à sua implementação. Em cenários regulados e colaborativos, onde a confiança entre partes não pode ser assumida a priori, a tecnologia blockchain oferece um arcabouço robusto para viabilizar operações auditáveis e resilientes. Contudo, é fundamental que sua adoção seja acompanhada de uma análise cuidadosa sobre os requisitos de desempenho e governança da rede, visando garantir sua viabilidade técnica e institucional a longo prazo.

9. Considerações Finais e Trabalhos Futuros

Este artigo apresentou uma proposta de arquitetura híbrida para Sistemas de Acesso ao Espectro (SAS) com integração à tecnologia de blockchain permissionada, visando atender aos requisitos de segurança, rastreabilidade, interoperabilidade e governança descentralizada em ambientes de compartilhamento dinâmico de espectro. A arquitetura proposta posiciona a blockchain como infraestrutura de comunicação entre instâncias SAS, mantendo os mecanismos operacionais locais já consolidados, e incorporando contratos inteligentes para automatização de processos e acordos entre operadores.

A análise dos requisitos funcionais da interface SAS-SAS demonstrou que a utilização de blockchain permissionada — especialmente com plataformas como o Besu — permite atender de forma robusta às necessidades de autenticação, troca de registros, sincronização temporal, recuperação por identificador, geração de *dumps* periódicos e notificações proativas, além de favorecer a conformidade regulatória e a transparência operacional.

A proposta se alinha às demandas emergentes das redes móveis 5G e 6G, em que a gestão dinâmica e segura do espectro torna-se ainda mais crítica. A arquitetura demonstrou potencial para oferecer uma base resiliente e auditável para o gerenciamento de recursos espectrais em redes densamente distribuídas e com múltiplos operadores, como se espera em cenários avançados de comunicação móvel.

Trabalhos futuros devem incluir avaliações quantitativas da arquitetura, utilizando testes de carga e simulações realistas de espectro dinâmico para medir sua escalabilidade e eficiência. Métricas como latência média de comunicação, *throughput* de transações blockchain, uso de CPU e memória nos nós SAS, *overhead* de replicação de dados e custo computacional para leitura e escrita de registros são importantes para validar o desempenho da solução em ambientes operacionais reais. Tais experimentos permitirão identificar gargalos, otimizar o desempenho da rede permissionada e garantir a viabilidade da adoção em larga escala.

Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), por intermédio da Chamada Pública No 068/2022, pela Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) projeto 2023/00811-0, projeto 2023/00673-7, projeto 2021/00199-8 (CPE SMARTNESS), projeto 2020/04031-1, e projeto 2018/23097-3, e também pelo Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD) e MCTI-Ministério da Ciência, Tecnologia e Inovação, com recursos financeiros do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (FUNTTEL) e administrados pela Financiadora de Estudos e Projetos (FINEP), no âmbito especificamente do projeto AERF - Ações Estratégicas para Redes Futuras, Contrato 01.22.0471.00, Referência 1508/22.

Referências

Alsaedi, W. K. et al. (2023). Spectrum options and allocations for 6g: A regulatory and standardization review. *IEEE Open Journal of the Communications Society*.

Google Cloud SAS Team (2025). Troubleshoot interoperability testing in the google sas portal. https://cloud.google.com/sas/docs/troubleshoot-interoperability. Acessado: 20 de Abril de 2025.

Li, Z., Wang, W., Guo, J., Zhu, Y., Han, L., and Wu, Q. (2021). Blockchain-assisted dynamic spectrum sharing in the cbrs band. In *IEEE ICCC*.

Li, Z., Wang, W., Wu, Q., and Wang, X. (2023). Multi-operator dynamic spectrum sharing for wireless communications: A consortium blockchain enabled framework. *IEEE Transactions on Communications*.

Perera, L., Ranaweera, P., Kusaladharma, S., Wang, S., and Liyanage, M. (2024). A survey on blockchain for dynamic spectrum sharing. *IEEE Open Journal of the Communications Society*, 5:1753–1770.

Salahdine, F., Han, T., and Zhang, N. (2023). 5g, 6g, and beyond: Recent advances and future challenges. *Annals of Telecommunications*, 78(9):525–549.

Scheid, E. J., Rodrigues, B. B., Killer, C., Franco, M. F., Rafati, S., and Stiller, B. (2021). Blockchains and distributed ledgers uncovered: Clarifications, achievements, and open issues. In *Advancing Research in Information and Communication Technology*, volume 600 of *IFIP Advances in Information and Communication Technology*, pages 289–317. Springer International Publishing.

Sousa, J. C., Duarte, V., Pinto, M., Evaristo, B., and Formigoni Filho, J. R. (2024). Solução descentralizada de compartilhamento de infraestrutura de redes baseada em blockchain. In *XLI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT 2024)*, Belém, PA, Brasil.

Wireless Innovation Forum (2016). Threat model for the citizens broadband radio service (cbrs). Version 1.0.0.

Wireless Innovation Forum (2020). Signaling protocols and procedures for citizens broadband radio service (cbrs): Spectrum access system (sas) - sas interface technical specification. Technical Report WINNF-TS-0096, Version 1.3.2, The Software Defined Radio Forum Inc.

Wireless Innovation Forum (2022a). Lessons learned from cbrs commercial deployments. White Paper.

Wireless Innovation Forum (2022b). Signaling protocols and procedures for citizens broadband radio service (cbrs): Spectrum access system (sas) - citizens broadband radio service device (cbsd) interface technical specification. Technical Report WINNF-TS-0016, Version 1.2.7, The Software Defined Radio Forum Inc.

Wu, Q., Wang, W., Li, Z., Zhou, B., Huang, Y., and Wang, X. (2023). Spectrumchain: a disruptive dynamic spectrum-sharing framework for 6g. *Science China Information Sciences*, 66(3):130302.

Xiao, Y., Shi, S., Lou, W., Wang, C., Li, X., Zhang, N., Hou, Y. T., and Reed, J. H. (2023). Bd-sas: Enabling dynamic spectrum sharing in low-trust environment. *IEEE Transactions*.