Sincronização Descentralizada entre Sistema de Acesso ao Espectro via Blockchain

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 a hybrid architecture for Spectrum Access Systems (SAS) that integrates permissioned blockchain technology to enable secure, auditable, and interoperable communication between different SAS instances. The solution replaces traditional REST interfaces with a distributed infrastructure based on smart contracts, which automate processes such as data usage agreements, device registration, and spectrum coordination. The proposal is validated through a prototype implemented with Hyperledger Besu, demonstrating practical feasibility and compliance with regulatory requirements. The architecture provides advantages such as data immutability, shared governance, and operational resilience, representing a step forward in secure and dynamic spectrum management for emerging mobile networks.*

Resumo. *Este artigo propõe uma arquitetura híbrida para Sistemas de Acesso ao Espectro (SAS), integrando a tecnologia de blockchain permissionada como infraestrutura para comunicação segura, auditável e interoperável entre diferentes instâncias SAS. A solução substitui as interfaces REST tradicionais por uma camada distribuída baseada em contratos inteligentes, responsáveis pela automação de processos como acordos de uso de dados, registro de dispositivos e coordenação de espectro. A viabilidade da proposta é demonstrada por meio de um módulo implementado com Hyperledger Besu, validando sua compatibilidade com requisitos regulatórios e operacionais. A arquitetura oferece benefícios como imutabilidade dos dados, governança compartilhada e resiliência frente a falhas, representando um avanço na gestão dinâmica e segura do espectro em redes móveis emergentes.*

1. Introdução

O avanço das redes móveis rumo às tecnologias 5G e 6G [Salahdine et al. 2023] exige um gerenciamento mais eficiente do espectro de radiofrequência, recurso limitado e essencial para a qualidade dos serviços [Alsaedi et al. 2023]. Nesse cenário, torna-se crucial o desenvolvimento de infraestruturas inteligentes capazes de lidar com mobilidade, baixa latência, alta densidade de dispositivos e reconfiguração dinâmica. O Sistema de Acesso ao Espectro (SAS – *Spectrum Access System*) surge como uma solução regulatória e tecnológica para o compartilhamento dinâmico do espectro, como exemplificado pelo modelo

CBRS nos Estados Unidos. No entanto, a comunicação entre instâncias SAS baseada em REST/HTTPS apresenta limitações em segurança, rastreabilidade, interoperabilidade e governança descentralizada, especialmente em ambientes heterogêneos e distribuídos.

Diante desse contexto, este trabalho busca responder à seguinte questão: *como garantir uma comunicação segura, auditável e interoperável entre SASs, alinhada aos requisitos das redes móveis emergentes, sem comprometer desempenho e conformidade regulatória?* A proposta consiste em uma arquitetura híbrida para SASs com integração de blockchain permissionada. Tal abordagem não substitui os mecanismos internos dos sistemas, mas adiciona uma camada de comunicação segura e confiável entre instâncias SAS. A tecnologia blockchain oferece autenticação forte, imutabilidade dos dados, rastreabilidade e automação via contratos inteligentes, atributos que respondem diretamente às exigências funcionais do gerenciamento inteligente do espectro.

As contribuições deste artigo abrangem a proposição de uma arquitetura baseada em blockchain para comunicação inter-SAS em redes 5G/6G, a análise da aderência dessa tecnologia aos requisitos da interface SAS-SAS, a descrição dos principais componentes, fluxos operacionais e aspectos de governança da arquitetura, além de um exemplo prático de implementação com Hyperledger Besu. Também são discutidas as vantagens, limitações e possibilidades de evolução da proposta, considerando o contexto de redes móveis de próxima geração e seus desafios regulatórios e técnicos.

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 Sistema de Acesso ao Espectro 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 explorado o uso de tecnologias blockchain como suporte ao gerenciamento dinâmico do espectro, especialmente no contexto do *Spectrum Access System* (SAS) e da banda CBRS. Essas iniciativas visam mitigar limitações associadas a modelos centralizados, como restrições de escalabilidade, segurança e confiabilidade.

No estudo de [Xiao et al. 2023], é proposta a arquitetura BD-SAS, que adota uma abordagem descentralizada com base em blockchain. Essa solução é estruturada em duas camadas: uma cadeia global (G-Chain), destinada à sincronização e funções regulatórias entre diferentes SASs, e cadeias locais (L-Chains), que realizam a gestão de espectro em áreas específicas. O modelo também incorpora mecanismos de *reshuffling* de servidores SAS para garantir resiliência contra falhas e resistir a ataques adaptativos. A proposta apresenta pontos de convergência com este trabalho, especialmente no aspecto da descentralização das decisões e na sincronização entre múltiplos SASs.

Li et al. [Li et al. 2023] propõem um *framework* que permite o compartilhamento dinâmico de espectro entre operadores distintos, utilizando uma blockchain de consórcio. A solução combina contratos inteligentes e um modelo de precificação baseado na teoria

dos jogos, especificamente o jogo de Stackelberg, proporcionando flexibilidade para que operadores atuem tanto como fornecedores quanto como solicitantes de espectro, conforme suas demandas. Embora o foco principal esteja no mercado entre operadores, os princípios de governança descentralizada e os mecanismos de incentivo oferecidos são igualmente aplicáveis ao contexto de SASs distribuídos.

O trabalho apresentado em [Wu et al. 2023] descreve o SpectrumChain, um *framework* voltado ao compartilhamento de espectro em ambientes 6G. A proposta utiliza uma blockchain hierárquica para registrar operações de alocação de espectro, assegurando a rastreabilidade das transações, além de integrar sensores cognitivos para suporte à tomada de decisão. Seu diferencial reside na escalabilidade e na adequação a cenários de redes heterogêneas emergentes.

A proposta B-CBRS, discutida em [Li et al. 2021], explora o uso de blockchain para coordenar o acesso ao espectro entre usuários da categoria *General Authorized Access*, delegando aos usuários *Priority Access* a responsabilidade pela gestão das alocações, realizada por meio de contratos inteligentes e algoritmos de otimização. Essa abordagem reforça a viabilidade de arquiteturas descentralizadas, mesmo considerando a hierarquia convencional dos modelos de acesso ao espectro.

Além dessas contribuições específicas, também se destacam estudos de caráter abrangente. Perera et al. [Perera et al. 2024] apresentam um *survey* que oferece uma análise detalhada sobre a aplicação de blockchain no gerenciamento dinâmico de espectro. O trabalho evidencia os principais benefícios, desafios e oportunidades associados, categorizando as soluções existentes com base na arquitetura adotada, nos modelos de sensoriamento e nas estratégias de acesso. Ademais, aponta lacunas e direções promissoras para pesquisas futuras, servindo como uma referência fundamental para o desenvolvimento de novas arquiteturas, como a proposta neste trabalho.

Diferentemente das abordagens anteriores, a arquitetura aqui proposta se concentra na aplicação de blockchain permissionada na interface SAS-SAS, proporcionando sincronização segura e auditável entre instâncias SAS. Além disso, aproveita as propriedades intrínsecas da tecnologia blockchain, como imutabilidade, controle refinado de acesso e automação por meio de contratos inteligentes.

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 2022]. Dentre suas funções críticas, destacam-se: a autorização de uso do espectro para dispositivos da rede CBRS; a proteção a usuários incumbentes, como radares navais; o gerenciamento de zonas de proteção, como as áreas PAL; e a coordenação de eventos regulatórios, incluindo a 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. Vista em Figura 1 e descritas a seguir.

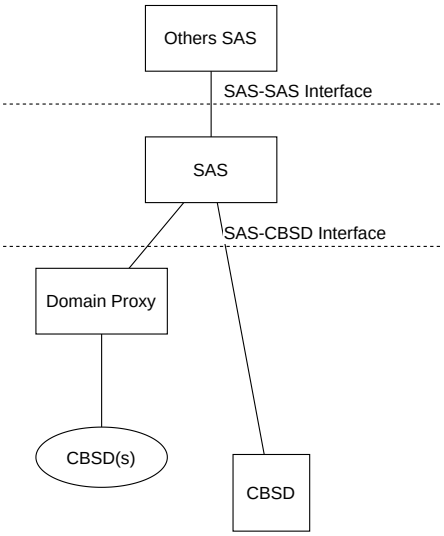

Figura 1. Protocolo das interfaces do SAS (adaptado de [Wireless Innovation Forum 2022]).

3.1. Interface SAS-CBSD

A interface SAS-CBSD estabelece o protocolo de comunicação entre o SAS e os dispositivos operando na banda CBRS, denominados CBSDs. Esse protocolo define os seguintes procedimentos operacionais:

- Registro inicial do CBSD no sistema;
- Consulta sobre disponibilidade de espectro na região de operação;
- Solicitação e emissão de permissões para uso de frequências;
- Envio de sinais periódicos (*Heartbeat*) para manter ativa a autorização;
- Procedimentos de renúncia e cancelamento do registro do dispositivo.

As mensagens trocadas seguem o formato JSON e são transmitidas sobre HTTPS, utilizando autenticação mútua baseada em certificados digitais X.509.

3.2. Interface SAS-SAS

A interface SAS-SAS tem como objetivo possibilitar a comunicação entre diferentes instâncias do SAS, garantindo interoperabilidade, consistência das informações e operação coordenada do sistema. Suas principais funcionalidades incluem:

- Sincronização de dados cadastrais de CBSDs, definição de zonas geográficas e eventos relacionados à coordenação espectral;
- Compartilhamento de informações provenientes dos sensores ESC (*Environmental Sensing Capability*);
- Coordenação de zonas de proteção e execução de ações vinculadas às exigências regulatórias;

- Implementação de mecanismos de transferência de dados via modelos *Push* e *Pull*.

A comunicação ocorre por meio de protocolos seguros, utilizando TLS versão 1.2 com autenticação mútua, assegurando confidencialidade, integridade e autenticidade das informações compartilhadas entre as diferentes instâncias do SAS.

4. Requisitos Funcionais da Interface SAS-SAS

Esta seção apresenta os requisitos funcionais essenciais para a implementação da interface de comunicação entre sistemas automatizados de gerenciamento dinâmico de espectro. Esses requisitos asseguram interoperabilidade, segurança e consistência na troca de informações entre SASs interconectados.

- **Segurança e Autenticação:** Toda comunicação entre SASs deve ser protegida por autenticação mútua utilizando TLS v1.2, com verificação rigorosa de certificados digitais. É obrigatória a negociação de *ciphersuites* robustas para garantir a confidencialidade, integridade e autenticidade dos dados. Conexões devem ser imediatamente encerradas em caso de falha no processo de autenticação.
- **Mecanismo de Descoberta de SASs:** A interface deve contemplar métodos tanto estáticos quanto dinâmicos para descoberta de SASs parceiros, empregando serviços como DNS ou DHCP. Além disso, é necessário permitir o registro e a manutenção dos *endpoints* de comunicação dos SASs descobertos.
- **Política de Uso dos Dados:** Antes de compartilhar informações, devem ser definidos acordos explícitos sobre os limites e condições de uso dos dados, assegurando alinhamento com regulamentações e diretrizes de privacidade aplicáveis.
- **Compartilhamento de Registros:** A interface precisa suportar a troca estruturada de registros que englobem: dispositivos CBSD; zonas protegidas (como PAL, PPA e zonas de exclusão); eventos de coordenação; sensores ESC; além de dados relacionados às instâncias SAS e seus respectivos operadores. Todos os registros devem possuir identificadores únicos, organizados hierarquicamente por meio de um sistema de *namespace*.
- **Mecanismos de Sincronização:** A interface deve permitir solicitações baseadas em intervalos de tempo (*time-range queries*) para obtenção de dados de CBSDs, zonas e eventos. Cada solicitação pode abranger no máximo 25 horas de registros, que devem ser retidos por um período mínimo de 30 dias. As respostas devem incluir exclusivamente registros que sofreram alterações dentro do intervalo solicitado, com possibilidade de aplicar filtros adicionais, como a seleção de CBSDs com autorizações ativas ou pendentes.
- **Consulta por Identificador:** Deve ser possível realizar consultas diretas a registros específicos utilizando seus identificadores únicos (*by-ID requests*), recuperando informações detalhadas de cada entidade.
- **Atualização via *Push*:** A interface deve possibilitar o recebimento de atualizações proativas (*Push*) contendo informações recentes sobre CBSDs, zonas e eventos. O SAS deve responder utilizando códigos HTTP apropriados, como 200 (sucesso), 422 (erro de validação) ou 50x (erros de servidor).
- **Geração de *Full Dumps*:** O SAS deve produzir, no mínimo a cada sete dias, um *Full Record Dump* abrangendo: CBSDs com *grants* ativos ou pendentes; zonas protegidas (incluindo PAL, PPA e zonas definidas ad hoc); e sensores ESC registrados. Esses arquivos devem estar disponíveis para acesso pelos SASs pares por, no mínimo, 14 dias.

- **Gestão dos Fluxos de Dados:** A interface deve oferecer suporte tanto para fluxos reativos (*Pull*, sob demanda) quanto proativos (*Push*). É essencial garantir robustez e continuidade das operações mesmo diante de falhas parciais de rede.

5. Aderência da Tecnologia Blockchain aos Requisitos Funcionais

A tecnologia blockchain oferece características que se alinham diretamente às necessidades funcionais dos sistemas de comunicação segura e auditável entre SASs. Esta seção discute como as propriedades fundamentais do blockchain podem ser aplicadas para atender aos requisitos apresentados.

Plataformas de blockchain permissionadas, como Hyperledger Fabric ou Besu, oferecem suporte nativo à autenticação mútua baseada em certificados digitais (e.g., X.509), combinada com comunicação segura via TLS v1.2. A integridade dos dados é garantida pela validação criptográfica dos blocos e transações. Além disso, mecanismos de controle de acesso podem ser implementados nos canais e redes do blockchain, assegurando que apenas entidades autorizadas participem da comunicação. A detecção de falhas na autenticação aciona, de forma automática, o encerramento das conexões TLS, complementado por monitoramento de eventos e revogação de credenciais.

Embora o blockchain não atue diretamente nos processos convencionais de descoberta dinâmica (como DNS ou DHCP), ele permite registrar, armazenar e compartilhar de forma imutável os dados de *endpoints* e relações entre SASs. A manutenção desses registros na blockchain garante rastreabilidade e integridade, fortalecendo a confiabilidade no estabelecimento e persistência das conexões entre pares.

Por meio de contratos inteligentes, é possível formalizar e automatizar acordos de uso de dados entre SASs. As regras contratuais ficam registradas de forma imutável na rede, e sua execução automática assegura conformidade com os termos definidos, permitindo auditoria transparente, rastreável e resistente a repúdios.

O blockchain pode ser utilizado como um repositório confiável e distribuído para o armazenamento e compartilhamento de informações relativas a CBSDs, zonas protegidas (como PAL, PPA e exclusões), sensores ESC e eventos de coordenação. Cada registro pode ser estruturado com identificadores únicos organizados em hierarquias via *namespace*, facilitando tanto a indexação quanto a recuperação eficiente dos dados.

A própria estrutura temporal do blockchain — onde cada transação é marcada por um *timestamp* — permite atender diretamente às demandas por sincronização baseada em intervalos de tempo. Consultas podem ser realizadas para recuperar registros alterados em janelas específicas, mantendo a integridade histórica dos dados. A retenção dos dados na rede blockchain naturalmente atende à exigência de disponibilidade mínima (ex.: 30 dias), e filtros personalizados podem ser implementados diretamente nos contratos inteligentes.

A busca por registros específicos utilizando identificadores únicos pode ser realizada por meio de métodos de consulta oferecidos pelos contratos inteligentes, garantindo acesso eficiente, preciso e imutável aos dados armazenados, sempre respeitando a hierarquia definida nos identificadores.

As operações do tipo *Push* podem ser representadas no blockchain como submissões de transações por entidades autorizadas. A confirmação de que a informação foi registrada com sucesso pode ser monitorada a partir da inclusão no bloco e da emissão de

eventos no contrato inteligente. Além disso, respostas podem ser modeladas com status análogos aos códigos HTTP (como 200 para sucesso, 422 para erro semântico, ou 50x para falhas internas).

A produção periódica de *Full Record Dumps* pode ser automatizada através de consultas que filtram o estado atual da blockchain, extraindo dados como CBSDs ativos, zonas protegidas e sensores ESC registrados. Esses conjuntos de dados podem ser disponibilizados tanto via APIs quanto por meio de repositórios descentralizados, garantindo sua acessibilidade por pelo menos 14 dias, conforme os requisitos estabelecidos.

Embora o blockchain não implemente diretamente os mecanismos de transporte de mensagens, ele é compatível com soluções baseadas em APIs REST sobre HTTPS/TLS, que utilizam JSON (RFC-7159) como formato de codificação. Isso assegura compatibilidade total com os protocolos já adotados na comunicação entre SASs.

O modelo distribuído do blockchain acomoda tanto fluxos reativos (*Pull*, via consultas aos registros existentes) quanto proativos (*Push*, mediante inclusão de novas transações). A replicação dos dados entre os nós da rede garante robustez operacional, assegurando continuidade mesmo em situações de falhas pontuais de infraestrutura.

Portanto, observa-se que o uso de blockchain contribui de forma significativa para aumentar a segurança, a transparência, a rastreabilidade e a automação no intercâmbio de informações entre SASs. Isso não apenas atende aos requisitos operacionais e regulatórios, como também oferece uma base resiliente e auditável para ambientes críticos que demandam alta integridade dos dados.

6. Arquitetura Proposta com Integração Blockchain

A Figura 2 ilustra a visão geral da arquitetura proposta, que integra uma rede blockchain permissionada ao funcionamento dos SASs. Nesta abordagem, o blockchain atua como uma camada de confiança para a comunicação segura, rastreável e auditável entre SASs, sem substituir os módulos operacionais internos do SAS.

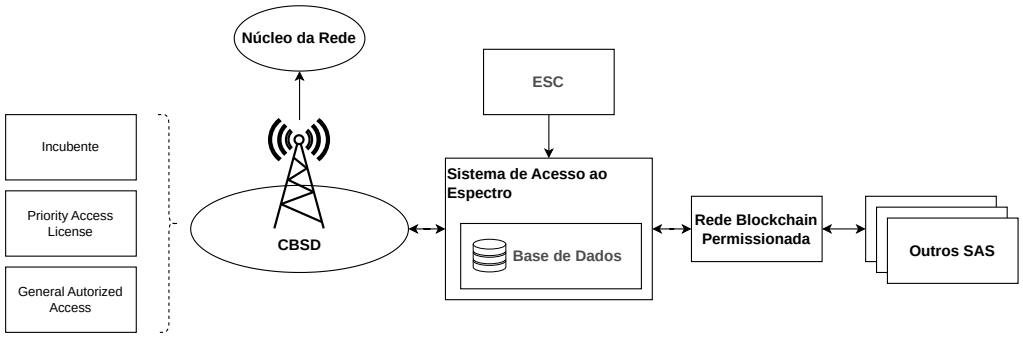

Figura 2. Arquitetura SAS integrada à Blockchain Permissionada.

6.1. Componentes Arquiteturais

A solução proposta é composta pelos seguintes componentes principais:

- **CBSD (Citizen Broadband Radio Service Device):** Dispositivo que opera no espectro dinâmico, reportando informações como localização, potência e demandas

espectrais ao SAS. Os CBSDs são classificados em três categorias — *Incumbentes*, PAL e GAA — que definem diferentes níveis de prioridade no uso do espectro, conforme as regras de compartilhamento da banda CBRS.

- **SAS (Spectrum Access System):** Sistema responsável pela gestão do uso do espectro, emissão de *grants* e pela comunicação tanto com os CBSDs quanto com outros SASs. Conta com uma base de dados local para decisões rápidas e armazenamento temporário das informações operacionais.
- **ESC (*Environmental Sensing Capability*):** Sistema de sensores dedicado à detecção de sinais de incumbentes, que auxilia o SAS na mitigação de interferências, especialmente em zonas sensíveis.
- **Rede Blockchain Permissionada:** Infraestrutura que suporta a comunicação oficial e segura entre SASs. Nesta rede, são armazenados registros referentes a CBSDs, zonas protegidas, *grants*, sensores ESC, eventos de coordenação e acordos de uso, assegurando transparência, segurança e rastreabilidade.
- **SASs Externos:** Outras instâncias SAS que interagem com o SAS local exclusivamente por meio da rede blockchain, eliminando a necessidade de canais externos tradicionais.

6.2. Fluxo Operacional

O funcionamento da arquitetura segue os seguintes passos operacionais:

1. O CBSD envia suas informações operacionais (como localização e necessidade de espectro) ao SAS local.
2. O SAS realiza uma verificação inicial em sua base de dados local para avaliar disponibilidade de espectro e aplicar políticas internas.
3. Quando necessário, o SAS acessa a blockchain para consultar informações como *grants* ativos, dados de coordenação ou registros de CBSDs operando na vizinhança.
4. A comunicação entre SASs ocorre exclusivamente via blockchain permissionada, utilizando contratos inteligentes para consultar dados por ID, executar sincronizações baseadas em intervalos temporais e registrar acordos e atualizações operacionais.
5. Operações como geração de *dumps* periódicos e envio de notificações (*push*) são implementadas como transações na blockchain, assegurando integridade e visibilidade compartilhada entre os SASs participantes.
6. Dados provenientes dos sensores ESC são processados localmente pelo SAS e, quando relevante, compartilhados com os demais SASs via blockchain.

6.3. Vantagens do Modelo Híbrido Integrado à Blockchain

A proposta mantém a estrutura tradicional de operação do SAS, com sua base de dados local e mecanismos de gerenciamento espectral, enquanto incorpora uma camada adicional baseada em blockchain para viabilizar uma comunicação inter-SAS mais segura, auditável e resiliente. Entre os principais benefícios desse modelo destacam-se:

- Aumento da transparência e rastreabilidade nas interações entre operadores SAS;
- Eliminação da dependência de APIs REST externas, reduzindo a superfície de ataque;

- Imutabilidade e auditoria nativa de todos os registros e transações;
- Execução automática de regras operacionais e contratos de dados via contratos inteligentes;
- Governança distribuída da rede blockchain, na qual os SASs atuam como nós validadores;
- Garantia de interoperabilidade por meio de contratos inteligentes padronizados e esquemas de dados comuns, permitindo a colaboração segura entre diferentes SASs.

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

A proposta aqui apresentada foi implementada como um módulo funcional dentro de uma solução descentralizada para compartilhamento de infraestrutura de redes suportada por tecnologia blockchain [Sousa et al. 2024]. Esse desenvolvimento é fruto de uma colaboração entre a Universidade Federal do Pará (UFPA) e o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD).

Para validar a aplicabilidade da arquitetura descrita, este exemplo prático demonstra a integração de um SAS com uma rede blockchain permissionada baseada no Hyperledger Besu. O ambiente simula uma rede composta por múltiplos SASs, cuja comunicação é inteiramente descentralizada, auditável e segura, utilizando a blockchain como meio oficial de interação e registro. A Tabela 1 lista as tecnologias utilizadas na construção deste protótipo.

Tabela 1. 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

Neste modelo, cada SAS mantém uma base de dados local que gerencia informações operacionais, incluindo registros de CBSDs, definição de zonas, análise de sensores ESC e tomada de decisões relativas à emissão de *grants*. Diferentemente das abordagens tradicionais, em que a comunicação entre SASs ocorre via interfaces diretas (como APIs REST), toda a troca de informações relevantes — como registros de dispositivos, atualizações de zonas, notificações de coordenação e acordos operacionais — é realizada por meio de transações na rede blockchain baseada no Besu[1].

A rede blockchain opera sob o mecanismo de consenso IBFT 2.0, apropriado para redes permissionadas que demandam alta disponibilidade, rápida finalização das transações e resiliência a falhas bizantinas. Cada instância SAS funciona como um nó validador,

[1] `https://besu.hyperledger.org/`

identificado por certificados X.509, garantindo autenticação mútua e controle distribuído de acesso. As operações fundamentais são modeladas através de contratos inteligentes desenvolvidos em Solidity, que encapsulam toda a lógica de leitura e escrita na blockchain.

O backend de cada SAS foi desenvolvido utilizando Node.js com o framework Express.js[2], enquanto a persistência local é realizada com PostgreSQL[3]. As interações com a blockchain, tanto para submissão de transações quanto para escuta de eventos, utilizam a biblioteca Web3.js[4]. Dessa forma, operações como registro de CBSDs, geração de *dumps* periódicos ou consultas diretas por identificadores são executadas diretamente sobre a infraestrutura blockchain.

Para assegurar transparência operacional e facilitar auditorias, o ambiente incorpora soluções de monitoramento baseadas em Prometheus[5] e Grafana[6]. Essas ferramentas monitoram métricas essenciais, como volume de transações, latência média na propagação de blocos, taxa de atualização entre SASs e desempenho geral da rede blockchain.

A escolha do Besu se deve, em parte, à sua compatibilidade com a *Ethereum Virtual Machine* (EVM), o que permite reaproveitamento de contratos inteligentes e integração facilitada com ferramentas existentes no ecossistema Ethereum. Além disso, sua interface JSON-RPC padronizada simplifica a integração com sistemas legados e soluções de monitoramento. Funcionalidades adicionais, como o uso do componente Tessera[7] para privacidade transacional, podem ser incorporadas em iterações futuras, possibilitando confidencialidade seletiva entre subconjuntos dos participantes da rede.

Esse exemplo demonstra que a adoção de uma blockchain como infraestrutura primária para comunicação entre SASs não apenas atende aos requisitos de segurança, rastreabilidade e integridade, como também estabelece uma base tecnológica robusta, escalável e interoperável para o gerenciamento dinâmico do espectro.

8. Discussão

O uso da tecnologia blockchain como meio de comunicação entre SASs traz uma série de vantagens, especialmente no que se refere à segurança, à rastreabilidade das operações e à promoção de uma governança descentralizada. Por outro lado, a adoção desse modelo também apresenta desafios técnicos e operacionais que precisam ser cuidadosamente avaliados. Esta seção analisa os principais pontos positivos e limitações associados ao uso da blockchain frente aos requisitos funcionais definidos.

Entre os benefícios mais relevantes está a garantia de imutabilidade dos dados registrados, proporcionando trilhas de auditoria robustas, fundamentais para assegurar a conformidade com normas regulatórias. A combinação de mecanismos nativos, como autenticação baseada em certificados digitais, assinaturas criptográficas e comunicação segura via TLS, fortalece significativamente a segurança no intercâmbio de informações entre SASs.

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

Adicionalmente, a capacidade de implementar regras operacionais, políticas de acesso e notificações diretamente em contratos inteligentes permite um alto grau de automação, eliminando ambiguidades e reduzindo a necessidade de intervenção manual nas operações. O modelo distribuído da blockchain também promove maior resiliência, assegurando que falhas isoladas em nós da rede não impactem a continuidade dos serviços — uma característica essencial para sistemas críticos, como os de gestão dinâmica do espectro.

Outro aspecto vantajoso, particularmente em blockchains permissionadas, é a possibilidade de controlar a visibilidade dos dados. Isso permite conciliar transparência nas operações compartilhadas com a preservação da confidencialidade de informações sensíveis, atendendo simultaneamente às exigências operacionais e regulatórias.

Apesar dos benefícios, o modelo blockchain impõe alguns desafios. A replicação completa dos dados em todos os nós da rede gera um aumento no consumo de recursos computacionais e de armazenamento, principalmente quando há necessidade de manter históricos extensos. A propagação de blocos e o tempo necessário para a confirmação de transações podem introduzir atrasos operacionais, o que é uma preocupação relevante em processos que exigem atualização quase em tempo real, como nas notificações sobre coordenação espectral.

A introdução dessa camada tecnológica exige também modificações na arquitetura dos sistemas existentes, bem como capacitação técnica das equipes responsáveis, tanto no desenvolvimento quanto na manutenção de contratos inteligentes e na operação dos nós validadores da blockchain. Outro ponto crítico está na definição de políticas claras para consenso, gestão de identidades e controle de acesso, especialmente quando envolve múltiplas organizações com diferentes interesses ou sob diferentes jurisdições.

Embora redes permissionadas ofereçam desempenho superior às blockchains públicas, ainda podem enfrentar limitações de escalabilidade, particularmente em cenários com altas taxas de transações e volumes significativos de dados. Diante disso, a decisão pela adoção de blockchain deve ser fundamentada em uma análise criteriosa que considere o equilíbrio entre os ganhos em segurança, rastreabilidade e governança, e os custos técnicos e operacionais envolvidos. Em ambientes regulados e colaborativos, onde a confiança entre as partes não pode ser presumida, a blockchain se posiciona como uma tecnologia capaz de sustentar operações seguras, auditáveis e resilientes. Contudo, sua implementação deve estar alinhada às demandas de desempenho, aos requisitos regulatórios e à governança da rede, garantindo sua sustentabilidade e eficácia no longo prazo.

9. Considerações Finais

Este artigo propôs uma arquitetura híbrida para Sistemas de Acesso ao Espectro (SAS), integrando tecnologia de blockchain permissionada para atender aos requisitos de segurança, rastreabilidade, interoperabilidade e governança descentralizada em cenários de compartilhamento dinâmico de espectro. A proposta utiliza a blockchain como camada de comunicação entre instâncias SAS, preservando os mecanismos operacionais locais e incorporando contratos inteligentes para automatizar processos e acordos entre operadores. A análise funcional da interface SAS-SAS demonstrou que a blockchain permissionada, especialmente com plataformas como o Hyperledger Besu, é capaz de atender a requisitos como autenticação, troca de registros, sincronização temporal, recuperação por

identificador, geração de *dumps* periódicos e notificações proativas, promovendo maior transparência e conformidade regulatória.

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 com o apoio do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel) e da Financiadora de Estudos e Projetos (Finep) — Ministério da Ciência, Tecnologia e Inovação.

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*.

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.

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 (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 (2022). 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*.