Uma Arquitetura Distribuída para Sistemas de Acesso ao Espectro com 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 presents a hybrid architecture for Spectrum Access Systems (SAS), incorporating permissioned blockchain as a secure, auditable, and interoperable communication infrastructure between different SAS instances. The proposed solution replaces conventional REST interfaces with a distributed layer based on smart contracts, which automates processes such as data-sharing agreements, device registration, and spectrum coordination. The architecture's feasibility is demonstrated through a functional prototype implemented with Hyperledger Besu, meeting regulatory and operational requirements. Key benefits include data immutability, decentralized governance, and fault resilience, representing a significant advancement in the dynamic and reliable management of spectrum in next-generation mobile networks.*

Resumo. *Este artigo apresenta uma arquitetura híbrida para Sistemas de Acesso ao Espectro (SAS), que incorpora blockchain permissionada como infraestrutura de comunicação segura, auditável e interoperável entre diferentes instâncias SAS. A proposta substitui interfaces REST convencionais por uma camada distribuída baseada em contratos inteligentes, que automatiza processos como acordos de compartilhamento de dados, registro de dispositivos e coordenação do espectro. A viabilidade da arquitetura é demonstrada por meio de um protótipo funcional implementado com Hyperledger Besu, atendendo a exigências regulatórias e operacionais. Entre os principais benefícios estão a imutabilidade dos dados, a governança descentralizada e a resiliência a falhas, caracterizando um avanço na gestão dinâmica e confiável do espectro em redes móveis de próxima geração.*

1. Introdução

O avanço das redes móveis rumo às tecnologias 5G e 6G [Salahdine et al. 2023] impõe novos desafios ao gerenciamento do espectro de radiofrequência, recurso escasso e essencial para a qualidade dos serviços [Alsaedi et al. 2023]. Torna-se, assim, necessário desenvolver infraestruturas inteligentes que atendam a requisitos como 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 para o compartilhamento dinâmico do espectro, adotada no modelo CBRS dos Estados Unidos.

No entanto, a comunicação entre SASs baseada em REST/HTTPS apresenta limitações em segurança, rastreabilidade e interoperabilidade. Este trabalho propõe uma arquitetura híbrida para SASs com integração à blockchain permissionada, que adiciona uma camada segura, auditável e automatizada por meio de contratos inteligentes, sem substituir os mecanismos internos dos sistemas legados.

Trabalhos recentes têm explorado o uso de blockchain para superar limitações dos modelos centralizados, como no BD-SAS [Xiao et al. 2023], que propõe cadeias globais e locais para coordenação e alocação de espectro; no *framework* multioperador de Li et al. [Li et al. 2023], com contratos inteligentes e modelos econômicos; no SpectrumChain [Wu et al. 2023], que combina sensores cognitivos e blockchain hierárquica; e no B-CBRS [Li et al. 2021], voltado à coordenação de acesso com base em contratos inteligentes. Um levantamento recente [Perera et al. 2024] mapeia essas soluções, destacando seus avanços e lacunas. A proposta deste artigo distingue-se por focar na interface SAS-SAS, utilizando blockchain permissionada para sincronização segura e interoperável entre instâncias regulatórias. As contribuições incluem a proposição de uma arquitetura distribuída com contratos inteligentes, análise de aderência aos requisitos, uma implementação prática com Hyperledger Besu e uma discussão sobre benefícios, desafios e direções futuras.

O artigo está estruturado da seguinte forma: a Seção 2 apresenta os requisitos da interface SAS-SAS; a Seção 3, a aplicação da blockchain; a Seção 4, a arquitetura proposta; a Seção 5, a implementação prática; a Seção 6, a análise crítica; e a Seção 7, as conclusões.

2. Requisitos Funcionais da Interface SAS-SAS

O Sistema de Acesso ao Espectro (SAS) é uma plataforma centralizada criada para gerenciar o uso dinâmico da faixa de 3550–3700 MHz no contexto do CBRS, nos Estados Unidos. Para garantir a coordenação eficiente e segura do espectro entre diferentes camadas de usuários — incluindo incumbentes, titulares de *Priority Access License* (PAL) e usuários de *General Authorized Access* (GAA) — o SAS depende de duas interfaces padronizadas: a SAS-CBSD, voltada à comunicação com os dispositivos finais, e a SAS-SAS, responsável pela interação entre instâncias SAS.

A interface SAS-SAS é essencial para assegurar interoperabilidade, consistência e segurança na comunicação entre sistemas distintos de gerenciamento de espectro. Para isso, deve atender a uma série de requisitos funcionais. Em primeiro lugar, a comunicação deve ser protegida por autenticação mútua via TLS v1.2, com uso de certificados digitais e *ciphersuites* seguras, encerrando conexões em caso de falhas de verificação. Também é necessário permitir a descoberta de SASs pares de forma estática ou dinâmica, mantendo registros atualizados dos *endpoints* de comunicação.

A troca de informações entre SASs deve seguir uma estrutura padronizada, incluindo dados sobre CBSDs, zonas protegidas, sensores ESC, eventos de coordenação e metadados administrativos, todos identificados de forma única. A interface deve oferecer suporte tanto a sincronizações por intervalo de tempo (limitadas a 25 horas e com retenção mínima de 30 dias) quanto a consultas diretas por identificador único. O intercâmbio de registros deve ocorrer por meio de fluxos *Push* e *Pull*, com respostas apropriadas e suporte a filtros específicos.

Além disso, é exigido que cada SAS gere *dumps* completos de registros ao menos uma vez por semana, mantendo-os disponíveis por pelo menos 14 dias para acesso pelos demais SASs. Esses mecanismos contribuem para a continuidade da operação mesmo em condições adversas, garantindo resiliência, confiabilidade e conformidade com os requisitos regulatórios do gerenciamento de espectro.

3. Aderência da Tecnologia Blockchain aos Requisitos Funcionais

A tecnologia blockchain apresenta características que contribuem diretamente para o atendimento dos requisitos funcionais da comunicação segura e auditável entre SASs. Infraestruturas permissionadas como Hyperledger Besu ou Fabric oferecem autenticação mútua baseada em certificados digitais e comunicação segura via TLS v1.2. A verificação criptográfica de transações garante integridade e confidencialidade, enquanto políticas de acesso e mecanismos de revogação asseguram controle e resposta a falhas de autenticação.

Embora a descoberta dinâmica de pares seja realizada externamente à blockchain, informações de registro e associação entre SASs podem ser armazenadas de forma imutável, garantindo rastreabilidade. Contratos inteligentes possibilitam a definição e aplicação automática de acordos de uso de dados, promovendo conformidade regulatória e auditoria transparente. A troca e sincronização de registros como CBSDs, zonas protegidas, sensores ESC e eventos regulatórios podem ser realizadas diretamente na blockchain, com identificadores únicos e estrutura hierárquica para facilitar a indexação. A presença de *timestamps* em transações permite consultas temporais, enquanto a recuperação por ID é viabilizada por funções de leitura nos contratos.

A troca de dados proativa (*Push*) pode ser modelada como transações submetidas por pares autorizados, com respostas automatizadas via contratos inteligentes. Da mesma forma, *dumps* periódicos podem ser extraídos com base em critérios definidos e disponibilizados por meio de APIs. Apesar da blockchain não especificar transporte e codificação de mensagens, integra-se facilmente a interfaces RESTful sobre HTTPS, compatíveis com JSON. Por fim, a blockchain suporta fluxos *Pull* e *Push*, com resiliência garantida pela replicação distribuída dos dados. Assim, sua adoção fortalece a confiança, rastreabilidade e automação na comunicação entre SASs, atendendo aos requisitos regulatórios e operacionais de ambientes distribuídos.

4. Arquitetura Proposta com Integração Blockchain

A Figura 1 apresenta a arquitetura proposta para integração de SASs com uma rede blockchain permissionada, utilizada como infraestrutura de confiança para a troca segura e auditável de informações, sem substituir os componentes internos dos SASs.

A arquitetura é composta por CBSDs (dispositivos que operam no espectro dinâmico), SASs (responsáveis pela coordenação e concessão de *grants*), sensores ESC (para detecção de incumbentes) e uma rede blockchain permissionada, que conecta diferentes SASs. Essa rede atua como meio oficial de troca de dados regulatórios, registros de CBSDs, zonas protegidas e eventos, promovendo segurança, rastreabilidade e automação por meio de contratos inteligentes. Toda comunicação entre SASs ocorre via blockchain, que também armazena notificações, *dumps* e acordos formais.

O fluxo operacional inicia com o envio de dados pelo CBSD ao SAS local, que consulta sua base interna e, quando necessário, interage com a blockchain para obter in-

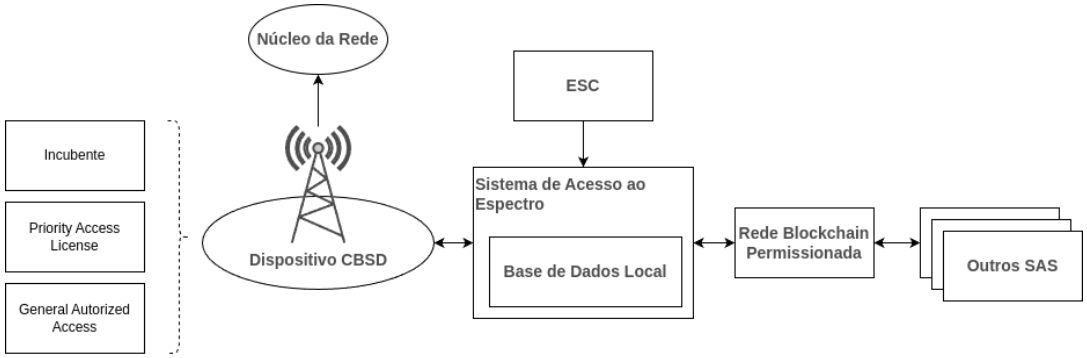

Figura 1. Arquitetura SAS com integração à Rede Blockchain Permissionada

formações sobre espectro, vizinhança ou eventos. Os SASs utilizam contratos inteligentes para registrar e consultar dados, automatizar acordos e emitir notificações. Dados de sensores ESC são avaliados localmente e podem ser compartilhados por meio da blockchain.

Esse modelo híbrido mantém a arquitetura tradicional dos SASs, mas adiciona uma camada robusta de comunicação inter-SAS. Entre os benefícios estão: transparência e rastreabilidade, eliminação de canais REST externos, imutabilidade e auditoria dos dados, e execução automatizada de políticas. A governança da rede blockchain é compartilhada entre os operadores SAS, que atuam como validadores, assegurando interoperabilidade por meio de contratos inteligentes padronizados.

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

A proposta foi implementada como um módulo dentro de uma solução descentralizada de compartilhamento de infraestrutura de redes baseada em blockchain [Sousa et al. 2024], fruto de uma parceria entre a Universidade Federal do Pará (UFPA) e o CPQD. Para demonstrar sua viabilidade, foi realizada uma implementação prática integrando um SAS à plataforma blockchain permissionada Hyperledger Besu. Nesta arquitetura, os SASs interagem exclusivamente por meio da blockchain, utilizando contratos inteligentes para garantir uma comunicação segura, auditável e distribuída.

Os principais componentes da solução incluem Besu com IBFT 2.0 como base blockchain, contratos escritos em Solidity, persistência local em PostgreSQL, lógica de aplicação em Node.js com Express, e monitoramento com Prometheus e Grafana. Cada SAS opera com base local para gerenciamento de CBSDs, zonas protegidas e sensores ESC, enquanto dados relevantes são publicados na blockchain, eliminando a necessidade de interfaces REST externas.

A blockchain atua como infraestrutura oficial para publicação de registros, emissão de *dumps*, consultas por ID e coordenação entre SASs. O mecanismo de consenso IBFT 2.0 garante finalização rápida e tolerância a falhas bizantinas. Operadores SAS atuam como validadores da rede, com autenticação por certificados X.509 e controle de acesso distribuído. O uso do Besu permite compatibilidade com a EVM, integração via APIs JSON-RPC e, futuramente, adoção de soluções de privacidade como Tessera.

A implementação demonstra que a integração da blockchain como camada de comunicação entre SASs atende aos requisitos de segurança, rastreabilidade e interoperabi-

lidade, ao mesmo tempo em que oferece uma base escalável e compatível com ambientes regulatórios e distribuídos para o gerenciamento dinâmico do espectro.

6. Discussão

A aplicação da tecnologia blockchain na comunicação entre SASs oferece benefícios importantes, especialmente em termos de segurança, rastreabilidade e governança descentralizada. A imutabilidade dos registros garante trilhas de auditoria confiáveis, reforçando a conformidade regulatória. Mecanismos como certificados digitais, assinaturas criptográficas e canais TLS asseguram a autenticidade e integridade das comunicações. Além disso, contratos inteligentes permitem a automação de regras operacionais, reduzindo ambiguidades e aumentando a eficiência dos acordos entre SASs. A replicação dos dados entre nós participantes assegura resiliência, mesmo em caso de falhas locais, e redes permissionadas permitem controle seletivo de acesso, equilibrando transparência e privacidade.

Por outro lado, a replicação de dados e o processamento distribuído podem implicar maior uso de recursos computacionais e latência na confirmação de transações, o que impacta aplicações sensíveis ao tempo. A adoção da blockchain exige alterações na arquitetura de sistemas legados, capacitação técnica e definição clara de políticas de identidade, consenso e permissão entre operadores, especialmente em ambientes multijurisdicionais. Embora blockchains permissionadas apresentem melhor desempenho que as públicas, limitações de escalabilidade ainda podem surgir em cenários de alto volume de dados. Assim, a adoção da blockchain deve ser cuidadosamente avaliada quanto ao custo-benefício, considerando os requisitos técnicos, regulatórios e institucionais do ambiente em que será aplicada.

7. Considerações Finais e Trabalhos Futuros

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.

Como perspectivas futuras, propõe-se a avaliação da arquitetura em cenários reais com múltiplos SASs, o uso de mecanismos de preservação de privacidade como Tessera, a integração com sistemas de *Network Slicing* e *Zero-Touch Network Management*, e a aplicação de técnicas de *machine learning* para análise proativa do espectro com base nos dados registrados. Também se destaca a possibilidade de estender a abordagem para interoperabilidade entre diferentes domínios regulatórios. Tais avanços poderão fortalecer um ecossistema mais seguro, confiável e escalável para o gerenciamento colaborativo do espectro, em consonância com as exigências das redes móveis 5G e 6G.

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.

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*.