18th International Conference on Development and Application Systems (DAS)
21-23 May 2026, Suceava, Romania, ISBN 979-8-3315-8387-3

HTTP security headers as a semantic policy layer for multichain interoperability

Ernest BÎTCA, Ana ȚURCAN, Ciprian DOBRE, Dumitru CIORBĂ

https://doi.org/10.1109/DAS69882.2026.11553307

Abstract

Multichain systems increasingly rely on web-based interfaces to expose services, including blockchain gateways, relayers, and wallet-facing applications. Existing interoperability solutions focus on protocol-level mechanisms, neglecting how services are accessed, combined, or isolated at the web interface. Reinterpreting HTTP security headers as a declarative semantic policy layer for multichain interoperability offers a pragmatic solution. Concepts of trust boundaries, isolation properties, and interaction constraints can be expressed through existing header semantics such as Content Security Policy (CSP), Cross-Origin Resource Sharing (CORS), Cross-Origin Opener Policy (COOP), Cross-Origin Embedder Policy (COEP), and Cross-Origin Resource Policy (CORP). To realize such a policy layer, we introduce a lightweight formal policy model and a Semantic Web Security Gateway (SWG) that composes and enforces header-based policies at the web edge, without modifying interoperability protocols. To illustrate how web-layer semantic policies complement native interoperability designs, we use a multichain application scenario. This highlights separation of concerns and supports a defense-in-depth approach.

Keywords: *multichain interoperability; semantic policy; web security*

References:

1. World Bank Group Information & Technology Solutions Technology & Innovation Lab, ‘ *Blockchain Interoperability* ’, World Bank Group, 2021. [Online]. Available: https://documents1.worldbank.org/curated/en/373781615365676101/pdf/Blockchain-Interoperability.pdf
Google Scholar

2. P. Zheng, Z. Jiang, J. Wu, and Z. Zheng, ‘ Blockchain-Based Decentralized Application: A Survey ’, *IEEE Open J. Comput. Soc.*, vol. 4, pp. 121–133, 2023, doi: 10.1109/OJCS.2023.3251854.
Google Scholar

3. I. Bashir, *Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3*, 1 st edn. Birmingham : Packt Publishing Limited, 2023.
Google Scholar

4. W. Li, Z. Liu, J. Chen, Z. Liu, and Q. He, ' Towards blockchain interoperability: a comprehensive survey on cross-chain solutions ', *Blockchain: Research and Applications*, vol. 6, no. 3, p. 100286, Sep. 2025, doi: 10.1016/j.bcra.2025.100286.
CrossRef Google Scholar

5. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ' A survey on the security of blockchain systems ', *Future Generation Computer Systems*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.
CrossRef Google Scholar

6. A. Augusto, R. Belchior, M. Correia, A. Vasconcelos, L. Zhang, and T. Hardjono, ' SoK: Security and Privacy of Blockchain Interoperability ', Nov. 29, 2023. doi: 10.36227/techrxiv.24595764.v4.
Google Scholar

7. World Wide Web Consortium (W3C), ' *Content Security Policy Level 3* ', W3C, 2026. [Online]. Available: https://www.w3.org/TR/CSP3/
Google Scholar

8. B. Adam, ' The Web Origin Concept ', *Internet Engineering Task Force (IETF), RFC 6454*, 2011. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6454.html
Google Scholar

9. NIST, ' NIST Special Publication 800-207: Zero Trust Architecture ', *National Institute of Standards and Technology*, 800–207, Aug. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207
CrossRef Google Scholar

10. World Wide Web Consortium (W3C), ' *Post-Spectre Web Development* ', 2021. [Online]. Available: https://www.w3.org/TR/post-spectre-webdev/
Google Scholar

11. ' *HTTP Security Headers and How They Work* ', Invicti. Accessed: Mar. 25, 2024. [Online]. Available: https://www.invicti.com/white-papers/whitepaper-http-security-headers/
Google Scholar

12. A. Zineddine et al., ' A systematic review of cybersecurity assessment methods for HTTPS ', *Computers and Electrical Engineering*, vol. 115, p. 109137, Apr. 2024, doi: 10.1016/j.compeleceng.2024.109137.
CrossRef Google Scholar

13. R. T. Fielding, M. Nottingham, and J. Reschke, ' HTTP Semantics ', *Internet Engineering Task Force (IETF), RFC 9110*, Jun. 2022. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9110.html
Google Scholar

14. ' *Content Security Policy - OWASP Cheat Sheet Series* '. Accessed: Mar. 13, 2024.

[Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
Google Scholar

15. L. Weichselbaum, M. Spagnuolo, S. Lekies, and A. Janc, ‘ CSP Is Dead, Long Live CSP! On the Insecurity of Whitelists and the Future of Content Security Policy ’, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna Austria : ACM, Oct. 2016, pp. 1376–1387. doi: 10.1145/2976749.2978363.
CrossRef Google Scholar

16. A. Țurcan and D. Ciorbă, ‘ Benchmarking Web Security for Countries in the Black Sea Region ’, in 2025 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Ruse, Bulgaria : IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CIEES66347.2025.11300099.
Google Scholar

17. E. Bîtca, ‘ *Multichain Document Registry* ’. 2026. [Online]. Available: https://github.com/ernest96/multichain-document-system
Google Scholar

18. E. Bîtca, ‘ *Multichain Grades Storage* ’. 2026. [Online]. Available: https://github.com/ernest96/multichain-grades-storage
Google Scholar

19. E. Bîtca, ‘ *Multichain Grades Storage–Live Demonstration* ’. 2026. [Online]. Available: https://grades.ernestbitca.com
Google Scholar

20. E. Bîtca, ‘ *Multichain Document Registry–Live Demonstration* ’. 2026. [Online]. Available: https://documents.ernestbitca.com
Google Scholar

21. Apache Software Foundation, ‘ *ab - Apache HTTP server benchmarking tool* ’. [Online]. Available: https://httpd.apache.org/docs/2.4/programs/ab.html
Google Scholar