

REFERENCES

- [1] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, “A survey on decentralized identifiers and verifiable credentials,” *IEEE Communications Surveys & Tutorials*, vol. 27, pp. 3641–3671, 2024.
- [2] H. Cui, M. Whitty, A. Miyaji, and Z. Li, “A blockchain-based digital identity management system via decentralized anonymous credentials,” *Proceedings of the 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure*, 2024.
- [3] K.-L. Tan, C.-H. Chi, and K.-Y. Lam, “Survey on digital sovereignty and identity: From digitization to digitalization,” *ACM Computing Surveys*, vol. 56, pp. 1 – 36, 2023.
- [4] E. Fathalla, M. Azab, C. Xin, and H. Wu, “Pt-ssim: A proactive, trustworthy self-sovereign identity management system,” *IEEE Internet of Things Journal*, vol. 10, pp. 17 155–17 169, 2023.
- [5] P. Herbke, A. Sapkota, and S. Lamichhane, “Lifecycle management of resumé with decentralized identifiers and verifiable credentials,” *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 1–3, 2024.
- [6] E. Samir, H. Wu, M. Azab, C. Xin, and Q. Zhang, “Dt-ssim: A decentralized trustworthy self-sovereign identity management framework,” *IEEE Internet of Things Journal*, vol. 9, pp. 7972–7988, 2022.
- [7] J. Hou, F. Wang, C. Wei, H. Huang, Y. Hu, and N. Gui, “Credibility assessment based byzantine-resilient decentralized learning,” *IEEE Transactions on Dependable and Secure Computing*, 2022.
- [8] M. M. Rashid, Y. Xiang, M. P. Uddin, J. Tang, K. Sood, and L. Gao, “Trustworthy and fair federated learning via reputation-based consensus and adaptive incentives,” *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 2868–2882, 2025.
- [9] F. Schardong and R. Custódio, “Self-sovereign identity: a systematic review, mapping and taxonomy,” *Sensors*, vol. 22, no. 15, p. 5641, 2022.
- [10] Y. Bai, H. Lei, S. Li, H. Gao, J. Li, and L. Li, “Decentralized and self-sovereign identity in the era of blockchain: A survey,” in *2022 IEEE international conference on Blockchain (Blockchain)*. IEEE, 2022, pp. 500–507.
- [11] H. Yildiz, A. Küpper, D. Thatmann, S. Göndör, and P. Herbke, “Toward interoperable self-sovereign identities,” *IEEE Access*, vol. 11, pp. 114 080–114 116, 2023.
- [12] C. N. Butincu and A. Alexandrescu, “Design aspects of decentralized identifiers and self-sovereign identity systems,” *IEEE Access*, vol. 12, pp. 60 928–60 942, 2024.
- [13] S. R. Garzon, H. Yildiz, and A. Küpper, “Decentralized identifiers and self-sovereign identity in 6g,” *IEEE network*, vol. 36, no. 4, pp. 142–148, 2022.

- [14] M. Babel, L. Willburger, J. Lautenschlager, F. Völter, T. Guggenberger, M.-F. Körner, J. Sedlmeir, J. Strüker, and N. Urbach, “Self-sovereign identity and digital wallets,” *Electronic Markets*, vol. 35, no. 1, p. 28, 2025.
- [15] Y. Yang, W. K. Ching, M. Huang, S. Innet, G. Yang, H. Pang, and R. H. Deng, “Disc: Decentralized identity system with self-sovereign credential aggregation,” *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 12 871–12 886, 2025.
- [16] Y. Jiang, H. Deng, Q. Wang, G. Yu, X. Wang, Y. Sai, S. Chen, W. Ni, and R. P. Liu, “Sok: Credential-based trust management in decentralized ledger systems,” in *2025 IEEE 24th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2025, pp. 1697–1706.
- [17] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, “A survey on decentralized identifiers and verifiable credentials,” *IEEE Communications Surveys & Tutorials*, 2025.
- [18] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, “Security, privacy, and decentralized trust management in vanets: A review of current research and future directions,” *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–39, 2024.
- [19] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jantti, “A survey on blockchain-based trust management for internet of things,” *IEEE Internet of Things Journal*, vol. 10, pp. 5898–5922, 2023.
- [20] R. Mukta, H. young Paik, Q. Lu, and S. Kanhere, “Credtrust: Credential based issuer management for trust in self-sovereign identity,” *2022 IEEE International Conference on Blockchain (Blockchain)*, pp. 334–339, 2022.
- [21] J. Yin, Y. Xiao, J. Feng, M. Yang, Q. Pei, and X. Yi, “Didtrust: Privacy-preserving trust management for decentralized identity,” *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 3105–3120, 2025.
- [22] G. D. Putra and B. R. O. Putra, “Endorsement-driven blockchain ssi framework for dynamic iot ecosystems,” in *2025 IEEE International Conference on Blockchain and Cryptocurrency*. IEEE, 2025, pp. 1–5.
- [23] R. A. Pava-Díaz, J. Gil-Ruiz, and D. A. López-Sarmiento, “Self-sovereign identity on the blockchain: Contextual analysis and quantification of ssi principles implementation,” *Frontiers in Blockchain*, vol. 7, p. 1443362, 2024.
- [24] E. Fathalla, M. Azab, C. Xin, and H. Wu, “Self-sovereign identity as a secure and trustworthy approach to digital identity management: A comprehensive survey,” *ACM Computing Surveys*, vol. 58, no. 7, pp. 1–47, 2026.
- [25] W. Tang, S. S. Mukherjee, S. Park, C. Chenli, H. Oh, J. Kim, and T. Jung, “Grac: graph-based anonymous credentials from identity graphs on blockchain,” in *2024 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2024, pp. 113–122.

- [26] Y. Yu, H. Yang, Y. Li, and R. H. Deng, "Calling out trustless users: A trust propagation scheme for decentralized trust management," *IEEE Transactions on Services Computing*, vol. 18, pp. 2646–2658, 2025.
- [27] B. Cai, X. Li, W. Kong, J. Yuan, and S. Yu, "A reliable and lightweight trust inference model for service recommendation in siot," *IEEE Internet of Things Journal*, vol. 9, pp. 10 988–11 003, 2022.
- [28] Y. Peng, J. Huang, and C. Li, "Dynatrac: A decentralized cross-domain authentication framework with dynamic reputation weighting and accountable tracing," *IEEE Internet of Things Journal*, vol. 12, pp. 39 955–39 970, 2025.
- [29] G. Liu, Z. Yan, D. Wang, H. Wang, and T. Li, "Deptvm: Decentralized pseudonym and trust value management for integrated networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, pp. 110–124, 2024.
- [30] J. Liu, Z. Liang, and Q. Lyu, "Empowering privacy through peer-supervised self-sovereign identity: Integrating zero-knowledge proofs, blockchain oversight, and peer review mechanism," *Sensors*, vol. 24, no. 24, p. 8136, 2024.
- [31] K. Chang and O. Seneviratne, "Zero-knowledge proof framework for identity verification and interoperable payments on the decentralized web," *ACM Transactions on the Web*, 2026.
- [32] A.-T. Hoang, C. Ileri, W. Sanders, and S. Schulte, "zkssi: A zero-knowledge-based self-sovereign identity framework," *2024 IEEE International Conference on Blockchain (Blockchain)*, pp. 276–285, 2024.
- [33] Z. Xing, Z. Zhang, Z. Zhang, Z. Li, M. Li, J. Liu, Z. Zhang, Y. Zhao, Q. Sun, L. Zhu *et al.*, "Zero-knowledge proof-based verifiable decentralized machine learning in communication network: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2025.
- [34] F. Piper, K. Wolf, and J. Heiss, "Privacy-preserving on-chain permissioning for kyc-compliant decentralized applications," *2025 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 1–10, 2025.
- [35] J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, "A zero-knowledge proof-enabled blockchain-based academic record verification system," *Sensors*, vol. 25, no. 11, p. 3450, 2025.
- [36] Y. Chen, Y. Zhang, X. Lin, T. Xu, Z. Pan, and L. Chen, "Zkp-capbac: Capability-based access control via on-chain zero-knowledge proofs for cross-domain hiding delegation tree," in *IEEE INFOCOM 2025-IEEE Conference on Computer Communications*. IEEE, 2025, pp. 1–10.
- [37] Y. Guo, X. Liu, K. Huang, W. Qu, T. Tao, and J. Zhang, "{DeepFold}: Efficient multilinear polynomial commitment from {Reed-Solomon} code and its application to zero-knowledge proofs," in *34th USENIX Security Symposium (USENIX Security 25)*, 2025, pp. 3497–3516.

- [38] X. Hu, X. Chen, Z. Dong, Y. Sun, Y. Guo, B. Fang, and J. Qi, “Optimized cross-chain transactions with aggregated zero-knowledge proofs: Enhancing efficiency and security,” *IEEE Internet of Things Journal*, vol. 12, no. 9, pp. 11 495–11 510, 2025.
- [39] K. Li, A. Lohachab, and V. Urovi, “Identity-private healthcare data sharing on blockchain via zero-knowledge proofs and account abstraction,” in *2025 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2025, pp. 1–10.
- [40] J. Liu, W. Wan, C. Long, J. Li, F. Yang, and Y. Fu, “Zkfdt: A fair exchange scheme for data trading based on efficient zero-knowledge proofs,” in *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2024, pp. 2197–2206.
- [41] J. Lauinger, S. Bezmez, J. Ernstberger, and S. Steinhorst, “Portal: Time-bound and replay-resistant zk proofs for single sign-on,” in *2024 IEEE International Conference on Blockchain*. IEEE, 2024, pp. 1–7.
- [42] C. Wiraatmaja and S. Kasahara, “Cost-efficient anonymous authentication scheme based on set-membership zero-knowledge proof,” *2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 1–8, 2023.
- [43] V. Femiak and K. Košťál, “Zero-knowledge proofs in anti-money laundering multi-party computation,” in *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2025, pp. 1–3.
- [44] H. Ma, Y. Liu, Y. Liu, F. Feng, and Z. Liu, “Dpczk: Enhancing device privacy through certificate-free encryption and zero knowledge proof in multi-domain iot environments,” *IEEE Internet of Things Journal*, 2025.
- [45] E. Fathalla, M. Azab, C. Xin, and H. Wu, “Self-sovereign identity as a secure and trustworthy approach to digital identity management: A comprehensive survey,” *ACM Computing Surveys*, 2025.
- [46] Y. Liu, B. Zhao, Z. Zhao, J. Liu, X. Lin, Q. Wu, and W. Susilo, “Ss-did: A secure and scalable web3 decentralized identity utilizing multilayer sharding blockchain,” *IEEE Internet of Things Journal*, vol. 11, pp. 25 694–25 705, 2024.
- [47] R. Xiong, W. Ren, X. Hao, J. He, and K. Choo, “Bdim: A blockchain-based decentralized identity management scheme for large scale internet of things,” *IEEE Internet of Things Journal*, vol. 10, pp. 22 581–22 590, 2023.
- [48] Q.-u.-A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, “Blockchain-based decentralized trust management in iot: systems, requirements and challenges,” *Complex & Intelligent Systems*, vol. 9, no. 6, pp. 6155–6176, 2023.
- [49] M. Deng, Y. Lyu, C. Yang, F. Xu, M. Ahmed, N. Yang, Z. Xu, and C. Ke, “Lightweight trust management scheme based on blockchain in resource-constrained intelligent iot systems,” *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 25 706–25 719, 2024.

- [50] J. Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, and D. Dou, "Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning," *Knowledge and Information Systems*, vol. 66, no. 8, pp. 4377–4403, 2024.
- [51] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity," *Information & Management*, vol. 59, no. 7, p. 103553, 2022.
- [52] Š. Čučko, V. Keršič, and M. Turkanović, "Towards a catalogue of self-sovereign identity design patterns," *Applied Sciences*, vol. 13, no. 9, p. 5395, 2023.
- [53] P. Bai, S. Kumar, G. Aggarwal, M. Mahmud, O. Kaiwartya, and J. Lloret, "Self-sovereignty identity management model for smart healthcare system," *Sensors*, vol. 22, no. 13, p. 4714, 2022.
- [54] M. M. Merlec and H. P. In, "Blockchain-based decentralized storage systems for sustainable data self-sovereignty: A comparative study," *Sustainability*, vol. 16, no. 17, p. 7671, 2024.
- [55] L. Perugini and A. Vesco, "On the integration of self-sovereign identity with tls 1.3 handshake to build trust in iot systems," *Internet of Things*, vol. 25, p. 101103, 2024.
- [56] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, 2024.
- [57] A. Grüner, A. Mühle, N. Lockenvitz, and C. Meinel, "Analyzing and comparing the security of self-sovereign identity management systems through threat modeling," *International journal of information security*, vol. 22, no. 5, pp. 1231–1248, 2023.
- [58] A. Farao, G. Papis, S. Panda, E. Panaousis, A. Zarras, and C. Xenakis, "Inchain: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain," *International Journal of Information Security*, 2023.
- [59] S. M. Mulaji and S. Roodt, "Factors affecting organisations' adoption behaviour toward blockchain-based distributed identity management: The sustainability of self-sovereign identity in organisations," *Sustainability*, vol. 14, no. 18, p. 11534, 2022.
- [60] L. Wei, Y. Yang, J. Wu, C. Long, and B. Li, "Trust management for internet of things: A comprehensive study," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7664–7679, 2022.
- [61] H. Amari, Z. Abou El Houda, L. Khoukhi, and L. H. Belguith, "Trust management in vehicular ad-hoc networks: Extensive survey," *Ieee Access*, vol. 11, pp. 47 659–47 680, 2023.
- [62] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang, "A semi-centralized trust management model based on blockchain for data exchange in iot system," *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 858–871, 2022.

- [63] M. Amiri-Zarandi, R. A. Dara, and E. Fraser, "Lbtlm: A lightweight blockchain-based trust management system for social internet of things," *The Journal of Supercomputing*, vol. 78, no. 6, pp. 8302–8320, 2022.
- [64] Z. Tu, H. Zhou, K. Li, H. Song, and Y. Yang, "A blockchain-based trust and reputation model with dynamic evaluation mechanism for iot," *Computer Networks*, vol. 218, p. 109404, 2022.
- [65] H. Han, M. Zhang, Z. Xu, X. Dong, and Z. Wang, "Decentralized trust management and incentive mechanisms for secure information sharing in vanet," *IEEE Access*, vol. 12, pp. 124 414–124 427, 2024.
- [66] M. U. F. Qaisar, W. Yuan, L. Zhang, S. A. Chaudhry, G. Han, and Y. Zhang, "A robust trust management system for v2x networks integrating isac with blockchain smart contracts," *IEEE Transactions on Network and Service Management*, 2026.
- [67] J. Chen, H. Yan, Z. Liu, M. Zhang, H. Xiong, and S. Yu, "When federated learning meets privacy-preserving computation," *ACM Computing Surveys*, vol. 56, no. 12, pp. 1–36, 2024.
- [68] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, "Privacy-preserving aggregation in federated learning: A survey," *IEEE Transactions on Big Data*, 2022.
- [69] A. Ozdemir and D. Boneh, "Experimenting with collaborative {zk-SNARKs}:{Zero-Knowledge} proofs for distributed secrets," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 4291–4308.
- [70] M. Kobelt, M. Sober, and S. Schulte, "A benchmark for different implementations of zero-knowledge proof systems," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 33–40.
- [71] O. Kuznetsov, A. Rusnak, A. Yezhov, D. Kanonik, K. Kuznetsova, and S. Karashchuk, "Enhanced security and efficiency in blockchain with aggregated zero-knowledge proof mechanisms," *IEEE access*, vol. 12, pp. 49 228–49 248, 2024.
- [72] M. Bellés-Muñoz, M. Isabel, J. L. Muñoz-Tapia, A. Rubio, and J. Baylina, "Circom: A circuit description language for building zero-knowledge applications," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 4733–4751, 2022.
- [73] Z. Wang, S. Chaliasos, K. Qin, L. Zhou, L. Gao, P. Berrang, B. Livshits, and A. Gervais, "On how zero-knowledge proof blockchain mixers improve, and worsen user privacy," in *Proceedings of the ACM Web Conference 2023*, 2023, pp. 2022–2032.
- [74] F. Baldimtsi, K. K. Chalkias, Y. Ji, J. Lindstrøm, D. Maram, B. Riva, A. Roy, M. Sedaghat, and J. Wang, "zklogin: Privacy-preserving blockchain authentication with existing credentials," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024, pp. 3182–3196.
- [75] Z. Liu, H.-Y. Lin, and Y. Liu, "Long-term privacy-preserving aggregation with user-dynamics for federated learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2398–2412, 2023.

- [76] G. C. Ismayilov and C. Özturan, “Trustless privacy-preserving data aggregation on ethereum with hypercube network topology,” *Computer Communications*, vol. 230, p. 108009, 2025.
- [77] G. Ismayilov and C. Özturan, “Ptts: Zero-knowledge proof-based private token transfer system on ethereum blockchain and its network flow based balance range privacy attack analysis,” *Journal of Network and Computer Applications*, vol. 233, p. 104045, 2025.
- [78] W. Serrano, “Verification and validation for data marketplaces via a blockchain and smart contracts,” *Blockchain: Research and Applications*, vol. 3, no. 4, p. 100100, 2022.
- [79] H. Taherdoost, “Smart contracts in blockchain technology: A critical review,” *Information*, vol. 14, no. 2, p. 117, 2023.
- [80] D. He, R. Wu, X. Li, S. Chan, and M. Guizani, “Detection of vulnerabilities of blockchain smart contracts,” *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12 178–12 185, 2023.
- [81] H. Wen, J. Stephens, Y. Chen, K. Ferles, S. Pailoor, K. Charbonnet, I. Dillig, and Y. Feng, “Practical security analysis of {Zero-Knowledge} proof circuits,” in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 1471–1487.
- [82] S. Pailoor, Y. Chen, F. Wang, C. Rodríguez, J. Van Geffen, J. Morton, M. Chu, B. Gu, Y. Feng, and I. Dillig, “Automated detection of under-constrained circuits in zero-knowledge proofs,” *Proceedings of the ACM on Programming Languages*, vol. 7, no. PLDI, pp. 1510–1532, 2023.
- [83] C. Wu, J. Xiong, H. Xiong, Y. Zhao, and W. Yi, “A review on recent progress of smart contract in blockchain,” *IEEE Access*, vol. 10, pp. 50 839–50 863, 2022.
- [84] J. Liang, D. Hu, P. Wu, Y. Yang, Q. Shen, and Z. Wu, “{SoK}: Understanding {zk-SNARKs}: The gap between research and practice,” in *34th USENIX Security Symposium (USENIX Security 25)*, 2025, pp. 2085–2104.
- [85] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, “Blockchain-enhanced zero knowledge proof-based privacy-preserving mutual authentication for iot networks,” *IEEE access*, vol. 12, pp. 118 618–118 636, 2024.
- [86] D. Shehada, A. Gawanmeh, C. Y. Yeun, and M. J. Zemerly, “Fog-based distributed trust and reputation management system for internet of things,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 8637–8646, 2022.
- [87] T. Gernot and C. Rosenberger, “Robust biometric scheme against replay attacks using one-time biometric templates,” *Computers & Security*, vol. 137, p. 103586, 2024.
- [88] Q. Hu, Y. Dai, S. Li, and T. Jiang, “Enhancing account privacy in blockchain-based iot access control via zero knowledge proof,” *IEEE Network*, vol. 37, no. 6, pp. 117–123, 2022.