References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf.

[2] H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, "A survey of state-of-the-art on blockchains: Theories, modelings, and tools," *ACM Computing Surveys (CSUR)*, vol. 54, no. 2, pp. 1–42, 2021.

[3] B.-J. Butijn, D. A. Tamburri, and W.-J. v. d. Heuvel, "Blockchains: A systematic multivocal literature review," *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–37, 2020.

[4] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[5] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[6] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, 2014.

[7] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot," *Journal of Network and Computer Applications*, vol. 149, p. 102 481, 2020.

[8] B. Cao, Z. Wang, L. Zhang, D. Feng, M. Peng, L. Zhang, and Z. Han, "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 353–385, 2023. DOI: 10.1109/COMST.2022.3204702.

[9] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain: A centralized tutorial," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–39, 2020.

[10] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Conference on the theory and application of cryptographic techniques*, Springer, 1987, pp. 369–378.

[11] *Delegated proof of stake (dpos)*, https://how.bitshares.works/en/master/technology/dpos.html, 2019.

[12] M. Castro, B. Liskov, *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, 1999, pp. 173–186.

[13] S. Islam, M. J. Islam, M. Hossain, S. Noor, K.-S. Kwak, and S. M. R. Islam, "A survey on consensus algorithms in blockchain-based applications: Architecture, taxonomy, and operational issues," *IEEE Access*, vol. 11, pp. 39 066–39 082, 2023. DOI: 10.1109/ACCESS.2023.3267047.

[14] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, no. 1, 2012.

[15] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[16] C. Sendner, H. Chen, H. Fereidooni, L. Petzi, J. König, J. Stang, A. Dmitrienko, A.-R. Sadeghi, and F. Koushanfar, "Smarter contracts: Detecting vulnerabilities in smart contracts with deep transfer learning.," in *NDSS*, 2023.

[17] C. Jentzsch, "Decentralized autonomous organization to automate governance," *White paper, November*, 2016.

[18] *A blockchain platform for the enterprise - hyperledger fabric*, https://hyperledger-fabric.readthedocs.io/en/release-2.5/, 2023.

[19] *The corda platform: An introduction*, https://corda.net/content/corda-platform-whitepaper.pdf, 2018.

[20] *Quorum - enterprise ethereum client*, https://goquorum.readthedocs.io/, 2019.

[21] M. Li, Y. Lin, J. Zhang, and W. Wang, "Cochain: High concurrency blockchain sharding via consensus on consensus," in *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications*, 2023, pp. 1–10. DOI: 10.1109/INFOCOM53939.2023.10228892.

[22] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[23] R. Han, J. Yu, H. Lin, S. Chen, and P. Esteves-Veríssimo, "On the security and performance of blockchain sharding," *Cryptology ePrint Archive*, 2021.

[24] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, vol. 10, pp. 93 039–93 054, 2022. DOI: 10.1109/ACCESS.2022.3200051.

[25] J. Poon and V. Buterin, "Plasma: Scalable autonomous smart contracts," *White paper*, pp. 1–47, 2017.

[26] Y. Liu, X. Xing, H. Cheng, D. Li, Z. Guan, J. Liu, and Q. Wu, "A flexible sharding blockchain protocol based on cross-shard byzantine fault tolerance," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2276–2291, 2023. DOI: 10.1109/TIFS.2023.3266628.

[27] A. Lohachab, S. Garg, B. Kang, M. B. Amin, J. Lee, S. Chen, and X. Xu, "Towards interconnected blockchains: A comprehensive review of the role of interoperability among disparate blockchains," *ACM Computing Surveys (CSUR)*, vol. 54, no. 7, pp. 1–39, 2021.

[28] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.

[29] J. Ping, Z. Yan, and S. Chen, "A privacy-preserving blockchain-based method to optimize energy trading," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1148–1157, 2023. DOI: 10.1109/TSG.2022.3198165.

[30] X. Hu, J. Yin, G. Cheng, J. Gong, L. Yang, H. Chen, and Z. Liang, "Verifying privacy-preserving financing orders on a consortium blockchain based on zk-snarks," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, 2022, pp. 1527–1532. DOI: 10.1109/WCNC51071.2022.9771773.

[31] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE symposium on security and privacy*, IEEE, 2014, pp. 459–474.

[32] V. Buterin, *Zk-snarks: Under the hood*, https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6, 2018.

[33] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali*, 2019, pp. 203–225.

[34] D. Mechkaroska, V. Dimitrova, and A. Popovska-Mitrovikj, "Analysis of the possibilities for improvement of blockchain technology," in *2018 26th Telecommunications Forum (TELFOR)*, 2018, pp. 1–4. DOI: 10.1109/TELFOR.2018.8612034.

[35] M. Basile, G. Nardini, P. Perazzo, and G. Dini, "Segwit extension and improvement of the blocksim bitcoin simulator," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 115–123. DOI: 10.1109/Blockchain55522.2022.00025.

[36] T. Neudecker and H. Hartenstein, "Short paper: An empirical analysis of blockchain forks in bitcoin," in *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*, Springer, 2019, pp. 84–92.

[37] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. bitcoin cash: Coexistence or downfall of bitcoin cash?" In *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 935–951. DOI: 10.1109/SP.2019.00075.

[38] A. N. Islam, M. Mäntymäki, and M. Turunen, "Why do blockchains split? an actor-network perspective on bitcoin splits," *Technological Forecasting and Social Change*, vol. 148, p. 119 743, 2019.

[39] X. Yi, Y. Fang, D. Wu, and L. Jiang, "Blockscope: Detecting and investigating propagated vulnerabilities in forked blockchain projects," in *NDSS*, 2023.

[40] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for iot," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, IEEE, 2018, pp. 1–6.

[41] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[42] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in iot: The challenges, and a way forward," *Journal of Network and Computer Applications*, vol. 125, pp. 251–279, 2019.

[43] Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-wsn," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[44] *Vital stats: Overview of road accidents in india*, https://www.prsindia.org/policy/vital-stats/overview-road-accidents-india, Accessed: 2017.

[45] *Road accidents in india 2020 report*, https://morth.nic.in/road-accident-in-india, Accessed: 2020.

[46] *Who report: Road traffic injuries*, https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries, Accessed: 2018.

[47] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, p. 100 182, 2019.

[48] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi, and W. Dou, "Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 1, pp. 1–17, 2021.

[49] J. Bao, D. He, M. Luo, and K.-K. R. Choo, "A survey of blockchain applications in the energy sector," *IEEE Systems Journal*, 2020.

[50] M. F. Munoz, K. Zhang, and F. Amara, "Zipzap: A blockchain solution for local energy trading," in *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2022, pp. 1–5. DOI: 10.1109/ICBC54727.2022.9805486.

[51] R. Myrzashova, S. H. Alsamhi, A. V. Shvetsov, A. Hawbani, and X. Wei, "Blockchain meets federated learning in healthcare: A systematic review with challenges and opportunities," *IEEE Internet of Things Journal*, pp. 1–1, 2023. DOI: 10.1109/JIOT.2023.3263598.

[52] S. H. Alsamhi, A. V. Shvetsov, S. V. Shvetsova, A. Hawbani, M. Guizani, M. A. Alhartomi, and O. Ma, "Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 328–338, 2023. DOI: 10.1109/TGCN.2022.3195479.

[53] Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: A review on the latest milestones of blockchain consensus algorithms," *Cybersecurity*, vol. 6, no. 1, p. 30, 2023.

[54] P. Vasin, "Blackcoin's proof-of-stake protocol v2," *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, vol. 71, 2014.

[55] M. Fitzi, P. Gazi, A. Kiayias, and A. Russell, "Proof-of-stake blockchain protocols with near-optimal throughput.," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 37, 2020.

[56] A. Kiayias, S. Quader, and A. Russell, "Consistency of proof-of-stake blockchains with concurrent honest slot leaders," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, 2020, pp. 776–786.

[57] V. Bagaria, A. Dembo, S. Kannan, S. Oh, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni, "Proof-of-stake longest chain protocols: Security vs predictability," in *Proceedings of the 2022 ACM Workshop on Developments in Consensus*, 2022, pp. 29–42.

[58] D. Karakostas and A. Kiayias, "Securing proof-of-work ledgers via checkpointing," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, 2021, pp. 1–5.

[59] M. Kohlweiss, V. Madathil, K. Nayak, and A. Scafuro, "On the anonymity guarantees of anonymous proof-of-stake protocols," in *2021 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2021, pp. 1818–1833.

[60] A. Song, Y. Dai, R. Ji, and Z. Song, "Extend pbft protocol with l-dag," in *2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2021, pp. 963–970. DOI: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00135.

[61] K. Antoniadis, J. Benhaim, A. Desjardins, E. Poroma, V. Gramoli, R. Guerraoui, G. Voron, and I. Zablotchi, "Leaderless consensus," *Journal of Parallel and Distributed Computing*, vol. 176, pp. 95–113, 2023.

[62] S. Liu, R. Zhang, C. Liu, C. Xu, and J. Wang, "An improved pbft consensus algorithm based on grouping and credit grading," *Scientific Reports*, vol. 13, no. 1, p. 13 030, 2023.

[63] Y. Xu and Y. Huang, "An n/2 byzantine node tolerate blockchain sharding approach," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020, pp. 349–352.

[64] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *25th {usenix} security symposium ({usenix} security 16)*, 2016, pp. 279–296.

[65] J. Liu, L. Yan, and D. Wang, "A hybrid blockchain model for trusted data of supply chain finance," *Wireless personal communications*, pp. 1–25, 2021.

[66] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[67] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.

[68] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2017, pp. 375–392.

[69] D. D. F. Maesa and P. Mori, "Blockchain 3.0 applications survey," *Journal of Parallel and Distributed Computing*, 2020.

[70] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)*, 2016, pp. 45–59.

[71] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th symposium on operating systems principles*, 2017, pp. 51–68.

[72] M. Tran, L. Luu, M. S. Kang, I. Bentov, and P. Saxena, "Obscuro: A bitcoin mixer using trusted execution environments," in *Proceedings of the 34th Annual Computer Security Applications Conference*, New York, NY, USA: Association for Computing Machinery, 2018, pp. 692–701.

[73] C. Li, P. Li, D. Zhou, Z. Yang, M. Wu, G. Yang, W. Xu, F. Long, and A. C.-C. Yao, "A decentralized blockchain with high throughput and fast confirmation," in *2020 {USENIX} Annual Technical Conference ({USENIX} {ATC} 20)*, 2020, pp. 515–528.

[74] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2018, pp. 583–598.

[75] J. Wang and H. Wang, "Monoxide: Scale out blockchains with asynchronous consensus zones," in *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, 2019, pp. 95–112.

[76] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of bft protocols," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 31–42.

[77] T. Crain, C. Natoli, and V. Gramoli, "Red belly: A secure, fair and scalable open blockchain," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 466–483.

[78] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18, Toronto, Canada: Association for Computing Machinery, 2018, pp. 931–948, ISBN: 9781450356930.

[79] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16, Vienna, Austria: Association for Computing Machinery, 2016, pp. 17–30.

[80] A. Mustafa, S. Alberto, B. Shehar, H. Dave, and D. George, "Chainspace: A sharded smart contracts platform," in *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*, USENIX, 2018. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018%5C_09-2%5C_Al-Bassam%5C_paper.pdf.

[81] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer pbft consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2021. DOI: 10.1109/TPDS.2020.3042392.

[82] G. A. Marson, S. Andreina, L. Alluminio, K. Munichev, and G. Karame, "Mitosis: Practically scaling permissioned blockchains," in *Proceedings of the 37th Annual Computer Security Applications Conference*, 2021, pp. 773–783.

[83] P. Gazi, L. Ren, and A. Russell, "Practical settlement bounds for proof-of-work blockchains," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 1217–1230.

[84] Z. Cai, J. Liang, W. Chen, Z. Hong, H.-N. Dai, J. Zhang, and Z. Zheng, "Benzene: Scaling blockchain with cooperation-based sharding," *IEEE Transactions on Parallel and Distributed Systems*, vol. 34, no. 2, pp. 639–654, 2022.

[85] B. Yu, H. Zhao, T. Zhou, N. Sheng, X. Li, and J. Xu, "Overshard: Scaling blockchain by full sharding with overlapping network and virtual accounts," *Journal of Network and Computer Applications*, vol. 220, p. 103 748, 2023.

[86] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3616–3630, 2020.

[87] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, "Prism: Deconstructing the blockchain to approach physical limits," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19, London, United Kingdom: Association for Computing Machinery, 2019, pp. 585–602, ISBN: 9781450367479.

[88] G. Wang, S. Wang, V. Bagaria, D. Tse, and P. Viswanath, "Prism removes consensus bottleneck for smart contracts," in *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, IEEE, 2020, pp. 68–77.

[89] L. Yang, V. Bagaria, G. Wang, M. Alizadeh, D. Tse, G. Fanti, and P. Viswanath, "Prism: Scaling bitcoin by 10,000 x," *arXiv preprint arXiv:1909.11261*, 2019.

[90] A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt, "Sok: Communication across distributed ledgers.," *Cryptology ePrint Archive*, vol. 12675, 2019.

[91] J. Kwon and E. Buchman, "A network of distributed ledgers," *Cosmos, dated*, pp. 1–41, 2018.

[92] H. Jin, X. Dai, and J. Xiao, "Towards a novel architecture for enabling interoperability amongst multiple blockchains," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, 2018, pp. 1203–1211.

[93] B. Pillai, K. Biswas, Z. Hóu, and V. Muthukkumarasamy, "Burn-to-claim: An asset transfer protocol for blockchain interoperability," *Computer Networks*, vol. 200, p. 108 495, 2021.

[94] H. Su, B. Guo, J. Y. Lu, and X. Suo, "Cross-chain exchange by transaction dependence with conditional transaction method," *Soft Computing*, pp. 1–16, 2022.

[95] M. Sigwart, P. Frauenthaler, C. Spanring, M. Sober, and S. Schulte, "Decentralized cross-blockchain asset transfers," in *2021 Third International Conference on Blockchain Computing and Applications (BCCA)*, Tartu, Estonia: IEEE, 2021, pp. 34–41.

[96] L. Besançon, C. F. Da Silva, and P. Ghodous, "Towards blockchain interoperability: Improving video games data exchange," in *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)*, IEEE, 2019, pp. 81–85.

[97] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, vol. 72, pp. 201–224, 2014.

[98] R. Zarick, B. Pellegrino, and C. Banister, "Layerzero: Trustless omnichain interoperability protocol," *arXiv preprint arXiv:2110.13871*, 2021.

[99] T. Xie, J. Zhang, Z. Cheng, F. Zhang, Y. Zhang, Y. Jia, D. Boneh, and D. Song, "Zkbridge: Trustless cross-chain bridges made practical," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 3003–3017.

[100] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, and Y.-C. Hu, "Hyperservice: Interoperability and programmability across heterogeneous blockchains," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 549–566.

[101] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[102] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for iot security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[103] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "Iot passport: A blockchain-based trust framework for collaborative internet-of-things," in *Proceedings of the 24th ACM symposium on access control models and technologies*, 2019, pp. 83–92.

[104] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale internet of things data storage and protection," *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 762–771, 2018.

[105] Y. Mirsky, T. Golomb, and Y. Elovici, "Lightweight collaborative anomaly detection for the iot using blockchain," *Journal of Parallel and Distributed Computing*, vol. 145, pp. 75–97, 2020.

[106] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019. DOI: 10.1109/JIOT.2018.2836144.

[107] C. H. Lau, K.-H. Y. Alan, and F. Yan, "Blockchain-based authentication in iot networks," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, IEEE, 2018, pp. 1–8.

[108] R. A. Michelin, A. Dorri, M. Steger, R. C. Lunardi, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "Speedychain: A framework for decoupling data from blockchain for smart cities," in *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2018, pp. 145–154.

[109] J. Gao, K. O.-B. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4278–4291, 2019.

[110] L. Zhang, M. Luo, J. Li, M. H. Au, K.-K. R. Choo, T. Chen, and S. Tian, "Blockchain based secure data sharing system for internet of vehicles: A position paper," *Vehicular Communications*, vol. 16, pp. 85–93, 2019.

[111] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[112] D. Zhang, F. R. Yu, and R. Yang, "Blockchain-based distributed software-defined vehicular networks: A dueling deep {q}-learning approach," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 4, pp. 1086–1100, 2019.

[113] X. Huang, C. Xu, P. Wang, and H. Liu, "Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE access*, vol. 6, pp. 13 565–13 574, 2018.

[114] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based vanet," *Information Sciences*, vol. 545, pp. 170–187, 2021.

[115] X. Feng, Q. Shi, Q. Xie, and L. Liu, "An efficient privacy-preserving authentication model based on blockchain for vanets," *Journal of Systems Architecture*, vol. 117, p. 102 158, 2021.

[116] Q. Mei, H. Xiong, Y. Zhao, and K.-H. Yeh, "Toward blockchain-enabled iov with edge computing: Efficient and privacy-preserving vehicular communication and dynamic updating," in *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, IEEE, 2021, pp. 1–8.

[117] S. Abbes and S. Rekhis, "A blockchain-based solution for reputation management in iov," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, 2021, pp. 1129–1134.

[118] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2018.

[119] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "Guardian: Blockchain-based secure demand response management in smart grid system," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 613–624, 2019.

[120] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1984–1992, 2019.

[121] T. Wang, J. Guo, S. Ai, and J. Cao, "Rbt: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration," *Applied Energy*, vol. 295, p. 117 056, 2021.

[122] Z. Guan, X. Lu, W. Yang, L. Wu, N. Wang, and Z. Zhang, "Achieving efficient and privacy-preserving energy trading based on blockchain and abe in smart grid," *Journal of Parallel and Distributed Computing*, vol. 147, pp. 34–45, 2021.

[123] J. Yang, A. Paudel, and H. B. Gooi, "Compensation for power loss by a proof-of-stake consortium blockchain microgrid," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3253–3262, 2020.

[124] Y. Cao, X. Ren, C. Qiu, X. Wang, H. Yao, and F. R. Yu, "A multi-agent reinforcement learning approach for blockchain-based electricity trading system," in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1–6. DOI: 10.1109/GLOBECOM46510.2021.9685510.

[125] J. Yang, A. Paudel, J. Dai, and H. B. Gooi, "A mining-rewarding mechanism for peer-to-peer energy trading blockchain," in *2021 IEEE PES Innovative Smart Grid Technologies-Asia (ISGT Asia)*, IEEE, 2021, pp. 1–5.

[126] S. Karumba, S. S. Kanhere, R. Jurdak, and S. Sethuvenkatraman, "Harb: A hypergraph-based adaptive consortium blockchain for decentralized energy trading," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14 216–14 227, 2022. DOI: 10.1109/JIOT.2020.3022045.

[127] T. AlSkaif, J. L. Crespo-Vazquez, M. Sekuloski, G. van Leeuwen, and J. P. S. Catalão, "Blockchain-based fully peer-to-peer energy trading strategies for residential energy systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 231–241, 2022. DOI: 10.1109/TII.2021.3077008.

[128] J. Ping, Z. Yan, and S. Chen, "A privacy-preserving blockchain-based method to optimize energy trading," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1148–1157, 2023.

[129] K. Christidis, D. Sikeridis, Y. Wang, and M. Devetsikiotis, "A framework for designing and evaluating realistic blockchain-based local energy markets," *Applied Energy*, vol. 281, p. 115 963, 2021.

[130] J. Guo, X. Ding, and W. Wu, "An architecture for distributed energies trading in byzantine-based blockchains," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 2, pp. 1216–1230, 2022.

[131] T. D. Nguyen and M. T. Thai, "A blockchain-based iterative double auction protocol using multi-party state channels," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 2, pp. 1–22, 2021.

[132] Z. Chen, W. Ding, Y. Xu, M. Tian, and H. Zhong, "Fair auctioning and trading framework for cloud virtual machines based on blockchain," *Computer Communications*, vol. 171, pp. 89–98, 2021.

[133] S. Singla, A. Dua, N. Kumar, and S. Tanwar, "Blockchain-based efficient energy trading scheme for smart-grid systems," in *2020 IEEE Globecom Workshops (GC Wkshps)*, IEEE, 2020, pp. 1–6.

[134] X. Ma, D. Xu, and K. Wolter, "Blockchain-enabled feedback-based combinatorial double auction for cloud markets," *Future Generation Computer Systems*, vol. 127, pp. 225–239, 2022.

[135] Y. Li, J. Wang, and H. Zhang, "A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces," *Journal of Network and Computer Applications*, p. 103 686, 2023.

[136] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*, 2017, pp. 1085–1100.

[137] E. Roth, D. Noble, B. H. Falk, and A. Haeberlen, "Honeycrisp: Large-scale differentially private aggregation without a trusted core (extended version)," Technical Report MS-CIS-19-03, University of Pennsylvania, Tech. Rep., 2019.

[138] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 17–30.

[139] S. K. Set and G. S. Park, "Service-aware dynamic sharding approach for scalable blockchain," *IEEE Transactions on Services Computing*, vol. 16, no. 4, pp. 2954–2969, 2023. DOI: 10.1109/TSC.2022.3231619.

[140] I. Grigg, "Eos-an introduction," *White paper. https://whitepaperdatabase. com/eos-whitepaper*, 2017.

[141] A. Yakovenko, "Solana: A new architecture for a high performance blockchain v0. 8.13," *Whitepaper*, 2018.

[142] D. Yaga, P. Mell, N. Roby, and K. Scarfone, *Blockchain technology overview*, https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf, 2018.

[143] E. Fujisaki and K. Suzuki, "Traceable ring signature," in *International Workshop on Public Key Cryptography*, Berlin, Heidelberg: Springer, 2007, pp. 181–200.

[144] B. C. Inc., *An open financial system on bitcoin (liquid network)*, https://blockstream.com/liquid/, [Online; accessed August-2022], 2022.

[145] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113, p. 101 883, 2021.

[146] Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, and N. Zheng, "Sbac: A secure blockchain-based access control framework for information-centric networking," *Journal of Network and Computer Applications*, vol. 149, p. 102 444, 2020.

[147] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, S. Mumtaz, and Z. ul Qayyum, "Docschain: Blockchain-based iot solution for verification of degree documents," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 3, pp. 827–837, 2020.

[148] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–32, 2020.

[149] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.

[150] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in vanets," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1779–1790, 2018.

[151] A. P. Sarr, P. Elbaz-Vincent, and J.-C. Bajard, "A new security model for authenticated key agreement," in *International Conference on Security and Cryptography for Networks*, Springer, 2010, pp. 219–234.

[152] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani, "Overcoming the key challenges to establishing vehicular communication: Is sdn the answer?" *IEEE Communications Magazine*, vol. 55, no. 7, pp. 128–134, 2017.

[153] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications," *IEEE Network*, vol. 34, no. 2, pp. 83–91, 2020.

[154] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets," *IEEE Access*, vol. 7, pp. 56 656–56 666, 2019.

[155] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, A. Pescape, M. Hasan, M. Sookhak, and A. Mosavi, "Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot," *IEEE Access*, vol. 9, pp. 28 361–28 376, 2021.

[156] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for vanets," *IEEE Access*, vol. 6, pp. 45 655–45 664, 2018.

[157] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iov paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.

[158] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[159] T. Coffey and P. Saidha, "Non-repudiation with mandatory proof of receipt," *ACM SIGCOMM Computer Communication Review*, vol. 26, no. 1, pp. 6–17, 1996.

[160] M. E. Peck and D. Wagman, "Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain," *IEEE Spectrum*, vol. 54, no. 10, pp. 56–61, 2017. DOI: 10.1109/MSPEC.2017.8048842.

[161] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys Tutorials*, vol. 19, pp. 446–464, 2017. DOI: 10.1109/COMST.2016.2627399.

[162] Y. Chen, W. Wei, H. Wang, Q. Zhou, and J. P. S. Catalão, "An energy sharing mechanism achieving the same flexibility as centralized dispatch," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3379–3389, 2021. DOI: 10.1109/TSG.2021.3060380.

[163] M. H. Ullah and J.-D. Park, "Distributed energy trading in smart grid over directed communication network," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3669–3672, 2021. DOI: 10.1109/TSG.2021.3067172.

[164] J. Guerrero, D. Gebbran, S. Mhanna, A. C. Chapman, and G. Verbič, "Towards a transactive energy system for integration of distributed energy resources: Home energy management, distributed optimal power flow, and peer-to-peer energy trading," *Renewable and Sustainable Energy Reviews*, vol. 132, p. 110 000, 2020.

[165] S. H. Alsamhi, F. A. Almalki, F. Afghah, A. Hawbani, A. V. Shvetsov, B. Lee, and H. Song, "Drones' edge intelligence over smart environments in b5g: Blockchain and federated learning synergy," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 295–312, 2022. DOI: 10.1109/TGCN.2021.3132561.

[166] T. Ha, D. Lee, C. Lee, and S. Cho, "Vcg auction mechanism based on block chain in smart grid," in *2021 International Conference on Information Networking (ICOIN)*, IEEE, 2021, pp. 465–468.

[167] H. T. Doan, J. Cho, and D. Kim, "Peer-to-peer energy trading in smart grid through blockchain: A double auction-based game theoretic approach," *Ieee Access*, vol. 9, pp. 49 206–49 218, 2021.

[168] D. Li, Q. Yang, W. Yu, D. An, Y. Zhang, and W. Zhao, "Towards differential privacy-based online double auction for smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 971–986, 2019.

[169] X. Hao, W. Ren, K.-K. R. Choo, and N. N. Xiong, "A self-trading and authenticated roaming scheme based on blockchain for smart grids," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4097–4106, 2022.

[170] S. Li, K. Xue, D. S. Wei, H. Yue, N. Yu, and P. Hong, "Secgrid: A secure and efficient sgx-enabled smart grid system with rich functionalities," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1318–1330, 2019.

[171] Q. Yang and H. Wang, "Privacy-preserving transactive energy management for iot-aided smart homes via blockchain," *IEEE Internet of Things Journal*, 2021.

[172] A. P. Ozisik and B. N. Levine, "An explanation of nakamoto's analysis of double-spend attacks," *Arxiv*, 2017. DOI: 10.48550/arXiv.1701.03977. eprint: https://arxiv.org/abs/1701.03977.

[173] M. El-Shehawey, "On the gambler's ruin problem for a finite markov chain," *Statistics & Probability Letters*, vol. 79, no. 14, pp. 1590–1595, 2009.

[174] H. Bao, B. Ren, B. Li, and Q. Kong, "Bbnp: A blockchain-based novel paradigm for fair and secure smart grid communications," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 12 984–12 996, 2022. DOI: 10.1109/JIOT.2021.3107301.

[175] I. Dimobi, M. Pipattanasomporn, and S. Rahman, "A transactive grid with microgrids using blockchain for the energy internet," in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, 2020, pp. 1–5.

[176] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash protocol specification," *GitHub: San Francisco, CA, USA*, vol. 4, p. 220, 2016.

[177] A. Al-Mamun and D. Zhao, "Echain: Securing electronic device provenance through privacy-preserving consortium blockchains," in *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, 2023, pp. 77–83. DOI: 10.1109/DSN-S58398.2023.00028.

[178] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings 7*, Springer, 2001, pp. 552–565.

[179] R. L. Rivest, L. Adleman, M. L. Dertouzos, *et al.*, "On data banks and privacy homomorphisms," *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978.

[180] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ser. ITCS '12, Cambridge, Massachusetts: Association for Computing Machinery, 2012, pp. 326–349, ISBN: 9781450311151. DOI: 10.1145/2090236.2090263.

[181] N. Bitansky, R. Canetti, A. Chiesa, S. Goldwasser, H. Lin, A. Rubinstein, and E. Tromer, *The hunting of the snark*, https://eprint.iacr.org/2014/580, 2014. [Online]. Available: https://eprint.iacr.org/2014/580.