A Tree-mapped Taxonomy of Blockchain Attacks

Emma Lubes and Justin M. Pelletier
Global Cybersecurity Institute
Rochester Institute of Technology
Rochester, NY USA
Corresponding author: jxpics@rit.edu

***Abstract*—Blockchains provide decentralized data storage and have gained popularity over the past decade. Their popularity has led to a multitude of attacks in research and practice. We analyzed the available literature and found 147 distinct blockchain attacks. We examined these blockchain attack vectors relative to existing blockchain attack taxonomies and found that current taxonomies miss one-third (33.33%) of attack types. We found that blockchain attacks are evolving faster than we can classify them according to conventional taxonomies. To address this, we provide a novel taxonomy of blockchain attacks using a treemap visualization. We believe this taxonomy will help the community understand the context for new attack discoveries and could help researchers better forecast opportunities for future work in blockchain security.**

***Index Terms*—attack taxonomy, attack treemap, blockchain attacks, blockchain attack vectors**

I. Introduction

Blockchain is a decentralized data structure in which peers, also called nodes, use a distributed ledger to record transactions. Peers come to a consensus about which data to add to the linked-node structure through a verification mechanism [1]. The most well-known consensus mechanism is Proof-of-Work. In this mechanism, blocks on the chain are linked together by a timestamp and a hash of the prior block's data. This process creates a data structure that provides security, anonymity, and integrity while retaining peer decentralization [2].

Paper organization - Section 2 discusses the background and significance of blockchain attack identification and classification. Section 3 reviews work related to blockchain attack taxonomies. Section 4 details the research procedures. Section 5 presents the research findings, Section 6 discusses and analyzes those findings, and Section 7 concludes the paper.

II. Background & Significance

The use of blockchain has grown very quickly since the introduction of Bitcoin in 2008. Ethereum, which is currently the most widely used blockchain implementation, records over 75,000 transactions daily [3]. Blockchain technology has been implemented in many industries, including medicine, economics, Internet of Things devices, and software engineering. It has also been discussed as a possible backbone for smart cities [4]. The rapidly-growing demand and use cases for blockchain systems and cryptocurrency over the past fourteen years means that cybersecurity too must learn to adapt and secure the technology, as it becomes incorporated into everyday life.

Attackers have already carried out several prominent cyber attacks on blockchain implementations. Among these are the DAO attack and the CoinDash hack [5]. Hackers stole roughly 7 million USD in the CoinDash attack, while the more costly DAO attack resulted in a loss of roughly 50 million USD. More high-profile cyber attacks are to come as well; Liu *et al* found that roughly 45% of Ethereum smart contracts contain embedded vulnerabilities [6]. As the attack surface for blockchain grows, so too must the cyber security knowledge base and infrastructure surrounding the technology.

III. Related Work

At the time of this paper's submission, there exist three taxonomies for blockchain attacks. Each taxonomy utilized a literature review to identify blockchain attacks, and two taxonomies focused on the most popular attacks at the time of publication. Each of the papers uses novel criteria to classify the attacks into a web or table structure, and each paper categorizes blockchain attacks based on different characteristics. The remainder of this section describes each of the taxonomies and their specific classification criteria.

Guggenberger *et al* use the literature review method to identify and categorize 87 known blockchain attacks [7]. The authors divide the attacks into six categories based on attack vectors. These categories are peer-to-peer network attacks, attacks against the consensus mechanism, attacks against the virtual machine or language, attacks against the on-chain application logic, attacks against the off-chain application logic, and attacks against the client application / wallet.

Dasgupta *et al* identify and classify 16 vulnerabilities within blockchain implementation [8]. The authors categorize attacks by vulnerability type rather than attack surface, as seen prior. Their eight categories are key attacks, identity attacks, manipulation attacks, service attacks, malware attacks, application attacks, reputation attacks, and quantum attacks. This approach results in some overlap between treating the attack categories strictly as categories versus treating the categories as attacks themselves. The authors also describe recent blockchain development trends and present potential countermeasures for some of the discussed attacks and corresponding vulnerabilities.

Anita and Vijayalakshmi identify and classify 25 vulnerabilities, also focused on blockchain implementation [9]. The authors classify attacks based on exploit type, rather than attack surface or vulnerability type. Their taxonomy identifies seven exploit type categories. These categories are hash-based attacks, centralization attacks, traffic attacks, network-level attacks, injection/insider attacks, integrity attacks, and private key leakage attacks.

IV. Research Design & Methods

In summary, we employed a systematic literature review followed by treemapping to generate the taxonomy. Treemapping is set of a well-established visualization techniques that can help make sense of hierarchical data [10]. This treemapping technique is ubiquitous across most application domains and represents a *de facto* standard in representing hierarchical data while simultaneously allowing additional visual variables per data element [11].

The remainder of this section provides details of our methods in each of three distinct procedural phases: 1) literature review, 2) attack identification and classification, and 3) taxonomy construction.

The first phase–a literature review–took place during the months of January and February in the year 2022. We found papers by searching Google Scholar for ”blockchain attacks”, ”blockchain attack vectors”, and ”blockchain security threats”. Papers did not have a maximum paper age. We only considered papers written in the English language and excluded all publications that were not peer-reviewed. During phase one, we found 86 relevant papers meeting these criteria.

The second phase consisted of attack identification and classification. This required a record entry for each attack mentioned in each paper, followed by the classification of each attack according to existing taxonomies. During this phase, we identified and attempted to classify 147 different attacks against the blockchain. We also noted attacks that did not fit into each taxonomy.

The third phase focused on building the blockchain attack taxonomy. We discarded six attacks listed within the taxonomies that did not appear during attack identification. We also discarded 17 attacks that did not have written descriptions and were only listed by name within the collected literature without substantive explanation. To systematize and contextualize the attacks, we wrote one-sentence descriptions of each attack. To further evaluate the attacks, we then established parent and/or child relationships between attacks based on collected literature and written descriptions, where those relationships existed. Of note, we found the treemap layout to be the optimal representation of our data and followed the general process for the *similarity-map layout* technique for the final visualization of our taxonomy, which corresponds to recent recommendations from Scheibel et. al's analysis of treemapping methods [11].

V. Findings

The literature review produced 86 papers that mentioned blockchain attacks by name. The keyword ”blockchain attack” provided 45 unique papers and ”blockchain security threats” yielded another 22 unique papers. A search for ”blockchain attack vectors” found 19 further unique papers. We identified 147 attacks on blockchain implementations and systems from these 86 papers. Table I considers these attacks by attack vector.

TABLE I
Attacks by Attack Vector

Attack Surface	**Number of Attacks**
Client Application / Wallet	24
Consensus Mechanism	38
On-Chain Application Logic	35
Off-Chain Application Logic	17
P2P Network	28
VM/Language	5

We then mapped the 147 attacks to the three existing blockchain attack taxonomies to find coverage rates, depicted in Table II. The coverage rates present the number of attacks we identified during the literature review which were present in each of the discovered existing blockchain attack taxonomies. The ”Not Covered” category covers the number of blockchain attacks that were not placed in any of the existing taxonomies by their authors. Finally, we determined children and parent relationships, listed in Appendix A, and constructed the visual representation as a treemap, depicted in Appendix B. These Appendices resulted in large graphics, which we make available at https://github.com/JP3L/BlockchainAttacks.

VI. Discussion

A. Common Attack Vectors

The most common attack vectors for blockchain attacks are attacks against the consensus mechanism and the on-chain application logic. These attacks make up approximately 50% (n=73) of the identified attacks. The second group of common attack vectors is attacks against the P2P network and the client application / wallet, comprising another 35% (n=52) of attacks. The third most utilized attack vector is off-chain application logic attacks, and the least utilized attack vector by far is VM/Language attacks. VM/Language attacks constitute only

TABLE II
Accuracy of Existing Taxonomies

Taxonomy	**# of Attacks**	**% of Attacks**
Not Covered	49	33.33%
Guggenberger *et al* [7]	81	55.10%
Dasgupta *et al* [8]	11	07.48%
Anita and Vijayalakshmi [9]	6	04.08%

3% (n=6) of the identified attacks. It is plausible that attackers avoid the off-chain application logic and VM/Language attack vectors as these types of attacks are highly dependent on the blockchain implementation and on operating third-party services; there are typically easier attacks that attackers can utilize to achieve their goals.

B. Attack Surface Expansion

Blockchain attacks are evolving faster than we can classify them. Blockchain is a relatively new technology that is popular and growing rapidly. The development rate of novel attacks reflects the rapid user-base growth. 33% (n=49) of the attacks identified in this paper are not covered in any of the three taxonomies, and 88% of the attacks are covered by one or less taxonomy. We found that most attacks are mentioned in only a few papers – representing novel attacks – and a large minority of attacks are not able to be covered by the available taxonomies. The poor attack coverage provided by the taxonomies is somewhat surprising because these taxonomies were created within the past five years using proven taxonomy construction methods. The inaccuracy of existing taxonomies suggests that the rate of blockchain attack surface expansion outpaces the community's ability to classify them.

C. Attack Evolution

We believe the treemap visualization depicted in Appendix A provides the best taxonomic potential for this quickly-expanding attack surface. A tree mapping encapsulates the living fluidity of attacks within its design, which provides a conceptual mitigation for some of the challenges that a traditional taxonomy faces.

Our attack tree consists of 147 nodes. Each node is presented via parent-child relationships identified during the literature review. The attack tree contains up to six degrees of these relationships. Each node is also categorized and color-coordinated by the attack vectors provided by Guggenberger *et al* [7]. We chose to display the attack vectors each attack utilizes to highlight how attacks can birth both new attacks within the same attack vector and can inspire or be combined to ¡spawn¿ new attacks in a different attack vector. By illustrating the familial relationships between blockchain attacks, our treemap systematically depicts the historical evolution of known attacks and provides a foundation for researchers to contextualize future attack discoveries.

D. Future Work

Our tree-mapping approach suggests that well-evolved attack types such as consensus mechanism and on-chain application logic attacks may continue to spawn novel discoveries. However, less-evolved attack vectors such as off-chain applications and client applications may have an equal or greater number of undiscovered attack potentials. Follow-on research could extend our attack surface visualization to consider differential rates of surface expansion as a potential indicator of attack types that are most ripe for evolution.

Also, our taxonomy does not include detection and protection mechanisms for each attack type. Such examination is beyond the scope of this work but is highly likely to find defensive gaps across one or more attack families.

VII. Conclusion

The use of blockchain has expanded rapidly, especially with the advent of digital currencies that rely on this technology. As blockchain use has increased, so has the number of blockchain attacks. Our examination of the available knowledge has found that current attack discoveries have mainly focused on consensus mechanisms and on-chain application logic attacks. We also found that blockchain attack surface expansion has outpaced our ability to systematically classify attacks and that the available taxonomies have become inaccurate. We therefore applied a treemap visualization to aid in contextualizing future attack surface discoveries. We believe our tree-mapped taxonomy will help blockchain security researchers 1) forecast evolution within branches of attack families, and 2) discover gaps in detection and protection mechanisms across classes of attack families.

VIII. Acknowledgements

This research was funded in part by ongoing activities in the SAFE Lab Pentesting Clinic at the Rochester Institute of Technology. J.M. Pelletier would also like to acknowledge the ongoing support he receives from the *Ordo Praedicatorum*.

References

[1] S. Soni and B. Bhushan, "A comprehensive survey on blockchain: Working, security analysis, privacy threats and potential applications," in *2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT)*, vol. 1. IEEE, 2019, pp. 922–926.

[2] H. Hasanova, U.-j. Baek, M.-g. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. 29, no. 2, p. e2060, 2019.

[3] 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, 2020.

[4] A. Davenport, S. Shetty, and X. Liang, "Attack surface analysis of permissioned blockchain platforms for smart cities," in *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2018, pp. 1–6.

[5] A. Averin and O. Averina, "Review of blockchain technology vulnerabilities and blockchain-system attacks," in *2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*. IEEE, 2019, pp. 1–6.

[6] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 254–269.

[7] T. Guggenberger, V. Schlatt, J. Schmid, and N. Urbach, "A structured overview of attacks on blockchain systems," in *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*, 2021.

[8] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *Journal of Banking and Financial Technology*, vol. 3, no. 1, pp. 1–17, 2019.

[9] N. Anita and M. Vijayalakshmi, "Blockchain security attack: a brief survey," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2019, pp. 1–6.

[10] L. McNabb and R. S. Laramee, "Survey of surveys (sos)-mapping the landscape of survey papers in information visualization," in *computer graphics forum*, vol. 36, no. 3. Wiley Online Library, 2017, pp. 589–617.

[11] W. Scheibel, D. Limberger, and J. Döllner, "Survey of treemap layout algorithms," in *Proceedings of the 13th international symposium on visual information communication and interaction*, 2020, pp. 1–9.

[12] I. M. Abdelwahed, N. Ramadan, and H. A. Hefny, "Cybersecurity risks of blockchain technology," *International Journal of Computer Applications*, vol. 177, no. 42, 2020.

[13] S. Aggarwal and N. Kumar, "Attacks on blockchain," in *Advances in Computers*. Elsevier, 2021, vol. 121, pp. 399–410.

[14] N. A. Akbar, A. Muneer, N. ElHakim, and S. M. Fati, "Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses," *Future Internet*, vol. 13, no. 11, p. 285, 2021.

[15] S. Al-Farsi, M. M. Rathore, and S. Bakiras, "Security of blockchain-based supply chain management systems: challenges and opportunities," *Applied Sciences*, vol. 11, no. 12, p. 5585, 2021.

[16] K. Alachkar and D. Gaastra, "Blockchain-based sybil attack mitigation: a case study of the i2p network," *August*, vol. 22, pp. 1–13, 2018.

[17] A. Alkhalifah, A. Ng, M. J. M. Chowdhury, A. Kayes, and P. A. Watters, "An empirical analysis of blockchain cybersecurity incidents," in *2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*. IEEE, 2019, pp. 1–8.

[18] A. Begum, A. Tareq, M. Sultana, M. Sohel, T. Rahman, and A. Sarwar, "Blockchain attacks analysis and a model to solve double spending attack," *International Journal of Machine Learning and Computing*, vol. 10, no. 2, pp. 352–357, 2020.

[19] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164 908–164 940, 2019.

[20] B. Bhushan, P. Sinha, K. M. Sagayam, and J. Andrew, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," *Computers & Electrical Engineering*, vol. 90, p. 106897, 2021.

[21] M. Brown, E. Peköz, and S. Ross, "Blockchain double-spend attack duration," *Probability in the Engineering and Informational Sciences*, vol. 35, no. 4, pp. 858–866, 2021.

[22] D. Chang, M. Hasan, and P. Jain, "Spy based analysis of selfish mining attack on multi-stage blockchain," *Cryptology ePrint Archive*, 2019.

[23] S.-Y. Chang, Y. Park, S. Wuthier, and C.-W. Chen, "Uncle-block attack: Blockchain mining threat beyond block withholding for rational and uncooperative miners," in *International Conference on Applied Cryptography and Network Security*. Springer, 2019, pp. 241–258.

[24] Y. Chen, H. Chen, M. Han, B. Liu, Q. Chen, and T. Ren, "A novel computing power allocation algorithm for blockchain system in multiple mining pools under withholding attack," *IEEE Access*, vol. 8, pp. 155 630–155 644, 2020.

[25] J. Cheng, L. Xie, X. Tang, N. Xiong, and B. Liu, "A survey of security threats and defense on blockchain," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30 623–30 652, 2021.

[26] V. Chia, P. Hartel, Q. Hum, S. Ma, G. Piliouras, D. Reijsbergen, M. Van Staalduinen, and P. Szalachowski, "Rethinking blockchain security: Position paper," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1273–1280.

[27] W. Cui, T. Dou, and S. Yan, "Threats and opportunities: Blockchain meets quantum computation," in *2020 39th Chinese control conference (CCC)*. IEEE, 2020, pp. 5822–5824.

[28] S. Dey, "A proof of work: Securing majority-attack in blockchain using machine learning and algorithmic game theory," *International Journal of Wireless and Microwave Technologies*, vol. 8, no. 5, pp. 1–9, 2018.

[29] L. Duan, Y. Sun, K. Zhang, and Y. Ding, "Multiple-layer security threats on the ethereum blockchain and their countermeasures," *Security and Communication Networks*, vol. 2022, 2022.

[30] G. Ebrahimpour, M. S. Haghighi, and M. Alazab, "Can blockchain be trusted in industry 4.0? study of a novel misleading attack on bitcoin," *IEEE Transactions on Industrial Informatics*, 2022.

[31] S. M. Emery, C. E. Chow, and R. White, "Penetration testing a us election blockchain prototype," *E-Vote-ID 2021*, p. 82, 2021.

[32] I. Fedotov and A. Khritankov, "Statistical model checking of common attack scenarios on blockchain," *arXiv preprint arXiv:2109.02803*, 2021.

[33] C. Gandhi, N. Shukla, G. Kaur, and K. Yadav, "Blockchain technology: Concept, applications, challenges, and security threats," in *Blockchain Applications in IoT Ecosystem*. Springer, 2021, pp. 77–104.

[34] E.-E. Gojka, N. Kannengießer, B. Sturm, J. Bartsch, and A. Sunyaev, "Security in distributed ledger technology: An analysis of vulnerabilities and attack vectors," in *Intelligent Computing*. Springer, 2021, pp. 722–742.

[35] S. Gong and C. Lee, "Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance," *Electronics*, vol. 9, no. 3, p. 521, 2020.

[36] N. Gupta, "Security and privacy issues of blockchain technology," in *Advanced Applications of Blockchain Technology*. Springer, 2020, pp. 207–226.

[37] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 341–390, 2020.

[38] M. Iqbal and R. Matulevičius, "Exploring sybil and double-spending risks in blockchain systems," *IEEE Access*, vol. 9, pp. 76 153–76 177, 2021.

[39] E. F. Jesus, V. R. Chicarino, C. V. De Albuquerque, and A. A. d. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," *Security and Communication Networks*, vol. 2018, 2018.

[40] M. Karpinski, L. Kovalchuk, R. Kochan, R. Oliynykov, M. Rodinko, and L. Wieclaw, "Blockchain technologies: Probability of double-spend attack on a proof-of-stake consensus," *Sensors*, vol. 21, no. 19, p. 6408, 2021.

[41] A. Kaushik, A. Choudhary, C. Ektare, D. Thomas, and S. Akram, "Blockchain—literature survey," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2017, pp. 2145–2148.

[42] M. Kedziora, P. Kozlowski, and P. Jozwiak, "Security of blockchain distributed ledger consensus mechanism in context of the sybil attack," in *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*. Springer, 2020, pp. 407–418.

[43] K. M. Khan, J. Arshad, and M. M. Khan, "Simulation of transaction malleability attack for blockchain-based e-voting," *Computers & Electrical Engineering*, vol. 83, p. 106583, 2020.

[44] N. Khoshavi, W. Francois, A. Sargolzaei, and H. Chintakunta, "A survey on blockchain security," in *2019 SoutheastCon*. IEEE, 2019, pp. 1–8.

[45] L. König, S. Unger, P. Kieseberg, S. Tjoa, and J. R. C. Blockchains, "The risks of the blockchain a review on current vulnerabilities and attacks." *J. Internet Serv. Inf. Secur.*, vol. 10, no. 3, pp. 110–127, 2020.

[46] T. Kumar, A. Braeken, V. Ramani, I. Ahmad, E. Harjula, and M. Ylianttila, "Sec-blockedge: Security threats in blockchain-edge based industrial iot networks," in *2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM)*. IEEE, 2019, pp. 1–7.

[47] A. Lazarenko and S. Avdoshin, "Financial risks of the blockchain industry: A survey of cyberattacks," in *Proceedings of the Future Technologies Conference*. Springer, 2018, pp. 368–384.

[48] X. Liang, S. Shetty, and D. Tosh, "Exploring the attack surfaces in blockchain enabled smart cities," in *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2018, pp. 1–8.

[49] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, and M. Laskowski, "Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack," *Journal of Cases on Information Technology (JCIT)*, vol. 21, no. 1, pp. 19–32, 2019.

[50] F. Moradi, A. Sedaghatbaf, S. A. Asadollah, A. Čaušević, and M. Sirjani, "On-off attack on a blockchain-based iot system," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2019, pp. 1768–1773.

[51] J. Munro, "Blockchain technology."

[52] C. Natoli and V. Gramoli, "The balance attack or why forkable blockchains are ill-suited for consortium," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2017, pp. 579–590.

[53] K. Nicolas, Y. Wang, G. C. Giakos, B. Wei, and H. Shen, "Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach," *IEEE Access*, vol. 9, pp. 3838–3857, 2020.

[54] H. Poston, "Mapping the owasp top ten to blockchain," *Procedia Computer Science*, vol. 177, pp. 613–617, 2020.

[55] D. Puthal, S. P. Mohanty, E. Kougianos, and G. Das, "When do we need the blockchain?" *IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 53–56, 2020.

[56] B. Putz and G. Pernul, "Detecting blockchain security threats," in *2020 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2020, pp. 313–320.

[57] G. Ramezan, C. Leung, and Z. J. Wang, "A strong adaptive, strategic double-spending attack on blockchains," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1219–1227.

[58] N. Rathod and D. Motwani, "Security threats on blockchain and its countermeasures," *Int. Res. J. Eng. Technol*, vol. 5, no. 11, pp. 1636–1642, 2018.

[59] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen, "Exploring the attack surface of blockchain: A systematic overview," *arXiv preprint arXiv:1904.03487*, 2019.

[60] T. Sato, M. Imamura, and K. Omote, "Threat analysis of poisoning attack against ethereum blockchain," in *IFIP International Conference on Information Security Theory and Practice*. Springer, 2019, pp. 139–154.

[61] S. Sayeed and H. Marco-Gisbert, "On the effectiveness of blockchain against cryptocurrency attacks," *Proceedings of the UBICOMM*, 2018.

[62] ——, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied sciences*, vol. 9, no. 9, p. 1788, 2019.

[63] ——, "Proof of adjourn (poaj): A novel approach to mitigate blockchain attacks," *Applied Sciences*, vol. 10, no. 18, p. 6607, 2020.

[64] M. A. Shahriar, F. H. Bappy, A. F. Hossain, D. D. Saikat, M. S. Ferdous, M. J. M. Chowdhury, and M. Z. A. Bhuiyan, "Modelling attacks in blockchain systems using petri nets," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2020, pp. 1069–1078.

[65] H. Shi, S. Wang, Q. Hu, X. Cheng, J. Zhang, and J. Yu, "Fee-free pooled mining for countering pool-hopping attack in blockchain," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 4, pp. 1580–1590, 2020.

[66] M. K. Shrivas, T. Y. Dean, and S. S. Brunda, "The disruptive blockchain security threats and threat categorization," in *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*. IEEE, 2020, pp. 327–338.

[67] M. K. Shrivas, T. Yeboah, and S. S. Brunda, "Hybrid security framework for blockchain platforms," in *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*. IEEE, 2020, pp. 339–347.

[68] S. T. Siddiqui, R. Ahmad, M. Shuaib, and S. Alam, "Blockchain security threats, attacks and countermeasures," in *Ambient Communications and Computer Systems*. Springer, 2020, pp. 51–62.

[69] S. K. Singh, M. M. Salim, M. Cho, J. Cha, Y. Pan, and J. H. Park, "Smart contract-based pool hopping attack prevention for blockchain networks," *Symmetry*, vol. 11, no. 7, p. 941, 2019.

[70] S. Singh, A. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network," *IEEE Access*, vol. 9, pp. 13 938–13 959, 2021.

[71] J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchain design for trusted decentralized iot networks," in *2018 13th Annual Conference on System of Systems Engineering (SoSE)*. IEEE, 2018, pp. 169–174.

[72] H. Sun, N. Ruan, and C. Su, "How to model the bribery attack: A practical quantification method in blockchain," in *European Symposium on Research in Computer Security*. Springer, 2020, pp. 569–589.

[73] P. Swathi, C. Modi, and D. Patel, "Preventing sybil attack in blockchain using distributed behavior monitoring of miners," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2019, pp. 1–6.

[74] S. Thakur and J. G. Breslin, "Collusion attack from hubs in the blockchain offline channel network," in *Mathematical Research for Blockchain Economy*. Springer, 2020, pp. 31–44.

[75] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*. IEEE, 2017, pp. 458–467.

[76] D. Valdeolmillos, Y. Mezquita, A. González-Briones, J. Prieto, and J. M. Corchado, "Blockchain technology: a review of the current challenges of cryptocurrency," in *International Congress on Blockchain and Applications*. Springer, 2019, pp. 153–160.

[77] T. R. Vance and A. Vance, "Cybersecurity in the blockchain era: a survey on examining critical infrastructure protection with blockchain-based technology," in *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*. IEEE, 2019, pp. 107–112.

[78] Y. Wang and G. Li, "Detect triangle attack on blockchain by trace analysis," in *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 2019, pp. 316–321.

[79] K. Wang, Y. Wang, and Z. Ji, "Defending blockchain forking attack by delaying mtc confirmation," *IEEE Access*, vol. 8, pp. 113 847–113 859, 2020.

[80] S. Wang, B. Yin, S. Zhang, Y. Cheng, L. X. Cai, and X. Cao, "A selfish attack on chainweb blockchain," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[81] P. Wei, Q. Yuan, and Y. Zheng, "Security of the blockchain against long delay attack," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2018, pp. 250–275.

[82] Z. Xing and Z. Chen, "Black bird attack: A vital threat to blockchain technology," *Procedia Computer Science*, vol. 199, pp. 556–563, 2022.

[83] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang, and L. Gao, "A lightweight and attack-proof bidirectional blockchain paradigm for internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4371–4384, 2021.

[84] R. Yang, X. Chang, J. Mišić, V. B. Mišić, and H. Kang, "On selfholding attack impact on imperfect pow blockchain networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 3073–3086, 2021.

[85] C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, "Analysis of security in blockchain: Case study in 51%-attack detecting," in *2018 5th International conference on dependable systems and their applications (DSA)*. IEEE, 2018, pp. 15–24.

[86] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and blockchain: Security and privacy," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 288–10 313, 2020.

[87] S. Zhang and J.-H. Lee, "Eclipse-based stake-bleeding attacks in pos blockchain systems," in *Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure*, 2019, pp. 67–72.

[88] S. Zhu, W. Li, H. Li, L. Tian, G. Luo, and Z. Cai, "Coin hopping attack in blockchain-based iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4614–4626, 2018.

[89] X. Zou, X. Deng, T.-Y. Wu, and C.-M. Chen, "A collusion attack on identity-based public auditing scheme via blockchain," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Springer, 2020, pp. 97–105.