2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)

Comprehensive overview on the deployment of machine learning, deep learning, reinforcement learning algorithms in Selfish mining attack in blockchain

1st M.J. Jeyasheela Rakkini
School of Computing
SASTRA Deemed University
Thanjavur, India
jeyasheelarakkini@cse.sastra.ac.in

2nd K. Geetha
School of Computing
SASTRA Deemed University
Thanjavur, India
geetha@cse.sastra.edu

2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon) | 978-1-6654-9790-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/MysuruCon55714.2022.9972484

***Abstract*— Blockchain, a disruptive technology, has many applications in the domain of Finance, banking, real estate, insurance, supply chain, gaming industry with much more plethora of applications in near future. In spite of the decentralized, distributed, transparent, tamper-proof, data-provenance nature of the blockchain, it is subject to a lot of security attacks such as forking attacks and block withholding attacks. One such attack under the forking attack is selfish mining, which targets the reward distribution and also the difficulty adjustment algorithms(DAA). An exhaustive surve is done on the existing approaches to detect selfish mining and also on the profitability of selfish mining attacks. This survey is organized particularly around the aspects of selection or exploration of the shortest branch of the blockchain when a fork occurs. We aim to identify the implications of selecting the shorter branch of the fork in the blockchain, especially after 2016 blocks, where a difficulty adjustment occurs. Our survey focuses on the deployment of machine learning and deep learning, reinforcement methods on mitigating the selfish mining attacks in the blockchain.**

Keywords*— *Selfish mining, Reinforcement learning, hash rate, Difficulty adjustment algorithms, forking attack.

I. Introduction

Satoshi [1] proposed a peer to peer money transaction system without the need for thirdparty or the intermediate party and also a way to mitigate the double spending attack in digital currency with blockchain architecture. Blockchain is a ledger of records backed up by hash functions. The records hold blocks of transactions and may be up to 1 MB in size. The inter block arrival time is 10 minutes in bitcoin blockchain and the block is mined by miners. Mining is the process of collecting the transactions from the mempool in the full node and solving a puzzle. Mining is done by the miners who have built a mining rig with CPU, GPU and ASIC and would be either doing solo mining or have joine the mining pools.

Colloborating with the miners in the mining pool and getting paid accordingly for the hash rate contribution is the prudent mining. There are some crypto farms who offer hash rate to mine cryptocurrencies for a rational rate.

Mining is the process of finding a target value or a nonce that when appended with the hash of the current block and hash of the previous block, results in a hash that is less than the target hash value given by the PoW system. The header of the block and the nonce are hashed repeatedly. Once the has value reduced below the threshold which is determined by the difficulty level in the Proof of Work (PoW) systems, the finding of target process will continue. PoW systems consume more electricity and have huge investment for their infrastructure. Proof of Stake consensus algorithms require only mild computational power, electricity and involves validators who stake their cryptocurrency Ether for the validation of transactions. There are many consensus algorithms and to design a consensus algorithm, is a interesting research insight. In Fig 1., illustrates the blocks in blockchain.

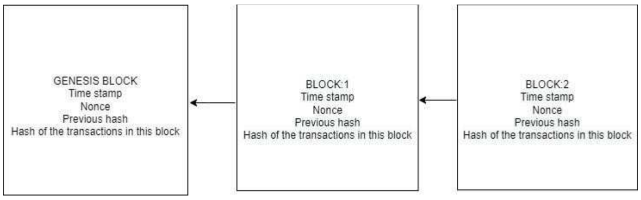
GENESIS BLOCK
Time stamp
Nonce
Previous hash
Hash of the transactions in this block
BLOCK:1
Time stamp
Nonce
Previous hash
Hash of the transactions in this block
BLOCK:2
Time stamp
Nonce
Previous hash
Hash of the transactions in this block

Fig. 1. The chaining of blocks in blockchain

The blocks have time stamp, previous block hash merkle hash of the current transactions in the current block and nonce. The full node has the full blockchain running with all the blocks, which amounts to massive data. Lightweight nodes have only the block headers and uses simplified payment verification method to verify the transactions. Bitcoin blockchain uses proof of work and Ethereum uses proof of stake for the consensus mechanisms. Crypto wallets are used to store the rewards of the miners.

Bitcoin mining involves finding a hash value that is equal to Hash (Nonce|| hash of transactions in current block|| hash of the previous block) < target value.. This will give a value of 256 bits.(||-append symbol). Hash rate is the computational power in MB/s used for verification of transactions and in the formation of new blocks. orphaned blocks are valid blocks that are rejected and are not in that major canonical blockchain. The availability of malicious activity in the blockchain mining is directly proportional to the orphaned blocks. Each block has time stamp, merkle tree of the transactions collected by the miner, in forming a block of one megabyte and hash of the previous block. Genesis block is the first block in the blockchain. Coinbase transaction in each block has the crypto address of the miners. In this crypto address, the miners get their mining rewards. Blockchain as a disruptive technology, has it's applications in plethora of domains such as finance, banking sector, logistics and supply chain management, health care sector, insurance, tracking of land assets and much more as given in Narayanan et al .[2]. In Fig 2., Selfish mining is

978-1-6654-9790-9/22/$31.00 ©2022 IEEE

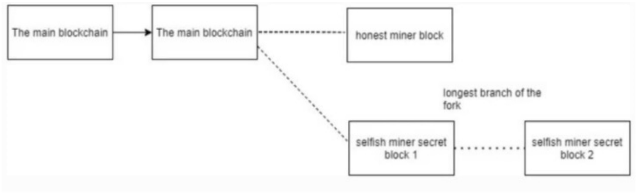
The main blockchain
The main blockchain
honest miner block
longest branch of the fork
selfish miner secret block 1
selfish miner secret block 2

Fig. 2. Selfish mining

shown with the branches of the fork from selfish miners and honest miners. Jeyasheela et al. [7] gives the exploration of the branch of the fork of honest miners, which is shorter than the branch of the selfish miners. The research directions in the blockchain are in designing new consensus mechanisms that are efficient than the existing algorithms, privacy and security preserving applications, data provenance applications in blockchain, federated machine learning algorithms and attack mitigation, detection strategies in blockchain who release two or more blocks at the same time when honest miners release a block, to earn more rewards. Reinforcement learning methods can be used to explore the profitability of the selfish miners, to select an optimal mining technique and also to mitigate the selfish mining attack. Henry et al. [3] discusses the privacy access methods of blockchain and to publish transactions anonymously in permissioned and permission less blockchain. n Fig 4., the previous papers have analyzed the profitability

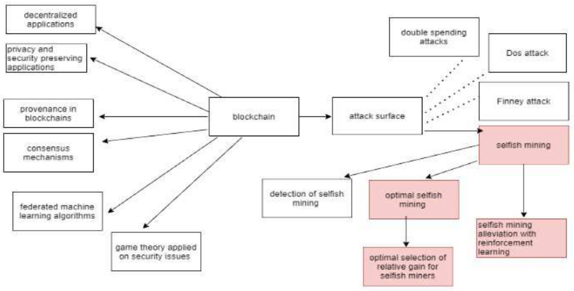
decentralized applications
privacy and security preserving applications
provenance in blockchains
consensus mechanisms
federated machine learning algorithms
game theory applied on security issues
blockchain
attack surface
double spending attacks
Dos attack
Finney attack
selfish mining
detection of selfish mining
optimal selfish mining
optimal selection of relative gain for selfish miners
selfish mining alleviation with reinforcement learning

Fig. 3. Selfish mining

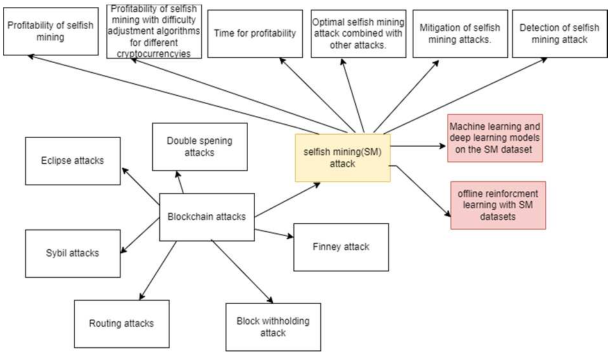
Profitability of selfish mining
Profitability of selfish mining with difficulty adjustment algorithms for different cryptocurrencyies
Time for profitability
Optimal selfish mining attack combined with other attacks.
Mitigation of selfish mining attacks.
Detection of selfish mining attack
Eclipse attacks
Double spening attacks
selfish mining(SM) attack
Machine learning and deep learning models on the SM dataset
offline reinforcment learning with SM datasets
Blockchain attacks
Sybil attacks
Finney attack
Routing attacks
Block withholding attack

Fig. 4. Taxonomy of Selfish mining attack

of selfish mining attacks with MDP simulators, profitability of selfish mining with different difficulty adjustment algorithms, the time for profitability, optimal selfish mining attack with the combination of other attacks such as Eclipse attack, mitigation of selfish mining attacks and detection of selfish mining attacks. The possibility of deploying deep learning models, machine learning models in selfish mining datasets has not been explored in full. With the selfish mining dataset, the possibility of offline reinforcement learning with SM datasets has not yet been explored. Prediction of the hash rate, classification of the hash rate, prediction of the rewards of the selfish miners are yet to be developed in machine learning and deep learning (ML/DL) approaches to selfish mining.

II. ATTACKS IN BLOCKCHAIN

A. *Double spending attack*

Double spending attack refers to the same amount of cryptocurrency spend frequently more than once. If an attacker can form the longest branch of the fork with the same cryptocurrency spent, on the other fork also, then it becomes a successful double spending attack. So one has to wait for 6 confirmations in blocks for a particular transaction to avoid double spending. Usman W et al.[4], explores in detail the accounting and auditability details in double spending problems with cryptocurrencies. Nicolas et al.[5], analyzed defensive strategies for selfish mining and double spending attack strategy with alert broadcasting, alert forwarding, inform about attack, detection of attack and conceptual research design about the attacks.

B. *Selfish mining attack*

Selfish mining attack also known as block with holding attack, is a strategy known to increase revenue of miners adapting this strategy, and to centralize bitcoin mining pools. Selfish miners stealthily mine blocks and form a private chain. When the private chain reaches an adequate size then the selfish miner releases its blocks, at the time the honest miners release their block, in order to create a fork. The longest fork is accepted and the selfish miners gain more rewards. There are two types of fork, one is hard fork. Hard fork is a radical upgrade that can make previous transactions and blocks either valid or invalid and requires all validators in a network to upgrade to a newer version. There is no backward compatibility and the validators have to validate the new chain. The other fork is soft fork. Soft fork is backward compatible, has validators in older version see the new version as valid. Soft fork will follow the new rules and will also honour the new rules.

III. MACHINE LEARNING METHODS APPLIED FOR BLOCK MINING REWARD PREDICTION

Blockchain powered by crypto currencies have voluminous real time data ,which can be used for prediction of block mining rewards, with machine learning and deep learning methods. Simon et al.[6] have implemented a k means clustering algorithm with Ethereum crypto miners who have unique crypto addresses and rewards. Clustering algorithms can be done with the datasets posted in http://xblock.pro/xblock- eth.html[7].The silhouette score of 71% is obtained for K- means clustering of miners with same rewards. Tao-Hung et al.[8] clusters the crypto addresses based on the patterns of transactions. The crypto addresses of the miners are classified as the address of the miners or as the address of the mining pools. The selfish mining attack is mitigated with upper confidence bound algorithm by Rakkini et al.[9]. Rakkini et al.[10] predicts the profitability of selfish mining attack with dash cryptocurrency blockchain and the corresponding DAA.

A. *Deep learning*

Prediciton of the crypto coin prices, decentralization trends in mining pools, hash rate classification of the miners, clustering of the miners who have same amount of input and output transactions are the potential problem statements for deep learning and machine learning with blockchain. Gas price optimization in Ethereum transactions is another problem that has vast potential for the usage of deep learning and machine learning algorithms. Simon et al.[6] uses keras classification model to identify the crypto addresses either mining pools or individual miners for binary classification problem. The upper confidence bound methodology has been used to elect the upcoming branch of the blocks to be included to the main blockchain when a fork occurs. This will mitigate selfish mining attacks after difficulty adjustment algorithm(DAA), where in previous works, selfish miners take over the mining process.

IV. Existing Methods

A. *How the longer chain is adapted*

Attacker fork the chain from the genesis block or when the difficulty level is low, and secretly mine the blocks and maintain a stealthy chain of blocks. The block time stamps are manipulated so that it gives an illusion that the block has been mined in the future. Difficulty adjustment algorithm has been manipulated owing to this selfish attack and the difficulty has been lowered. Below are the papers that are explored in selfish mining, for the detection of selfish mining, profitability of selfish mining with respect to their revenue and the reward distribution mechanisms.

V. Reinforcement Learning Algorithms With Selfish Mining

Most of the previous papers have focused on selfish mining attack detection and mitigation. This paper focusses on the selection of the shortest branch when a fork occurs after the initial difficulty adjustment algorithm. The longest branch of the fork of the selfish miners gets selected, according to the protocol of the blockchain. At this stage γ hash rate of rational honest miners would drift from honest mining pools and mine ahead selfish mining pool's block for more block rewards and this will increase the selfish mining attack. This is the basic model of selfish mining as given in [18]. Since the fork occurs mainly due to selfish mining activities, any reinforcement learning that gives the optimal attack parameters for mitigating the attack or for increasing the relative gain, the revenue of the miners would be of utmost importance.

Wang, Z., et al.[32], analysed the profitability of selfish mining with a higher mining power and the attackers can optimize their rewards with scrutinizing attack strategies. Charlie Hou et al.[33],explores optimal selfish mining attack in bitcoin blockchain, Nash equilibrium in block withholding attacks and a partially observed Markov game with multi agents is devised with SquirRL framework. Here the multi agents are selfish miners. A deep reinforcement learning is used to analyze attacks on the incentive mechanisms of blockchain. Yang, Guoyu et al.[34], uses reinforcement learning strategy to learn a mining strategy dynamically by interacting with the network. Liu et al.[35] uses blockchain enabled deep reinforcement learning to a secure and reliable data sharing among mobile terminals. Lu, Cong, et al.[36], analyzes about offline reinforcement learning from visual observations, with continuous actions spaces. In offline reinforcement learning, the objective is to maximize a policy that maximizes expected discount return, through interactions with the environment. Model based and model free environments are deployed in offline reinforcement learning. Shi, Laixi, et al.[37] analyzes offline reinforcement learning for learning an optimal policy using history data without active exploration of the environment.

TABLE I. COMPREHENSIVE SURVEY ON THE SELFISH MINING

Authors	Strategy	Method used	Advantages	Limitations and Future work
Davidson, M.et al. [11]	Various adjustment algorithms are managed by the profitability of selfish mining algorithms	Profitability of Selfish mining	Suggestion of parameter sets that would improve the DAA algorithms resilience against selfish mining	Combinations of different DAA can be tried
Eijkel. D. et al.[12]	Detection of selfish mining	The Block publishing height model along with the Transaction confirmation height model also uded	Network wide defense mechanism to disincentivize selfish miners	No method had been devised to fond the re-org attack and also to find the number of blocks that are reorganized.
Gober, J.A. et al.[13]	Revenue model of the Blockchain which focusses on the profitability of the miners.	The hash rate of the multiple selfish miners, speed of propagation of the blocks mined by them is considered.	Selfish mining is favorable for miners with certain threshold of hashing power, with other network conditions in his/her favor.	True dynamics of such a network has not been explored. Classification of the hash rate of those multiple selfish miners can be explored.
Zhang .R et al.[14]	Fork resolving policy	Block that has links to the competing block of their predecessor is accepted.	The hash of the uncle block has to be embedded in the valid in time block for it be appended as next block.	Incentive compatibility for the blocks who have embedded the hash of the uncle block can be devised.
Grunspan, C et al.[15]	Profitability of selfish mining	Honest miner's attraction to selfish mining pools after the first DAA is explored.	The honest miner when he joins the selfish mining pool after the initial DAA increases the relative profit of the pool	The attack vector of withdrawing from the network, switching mining from one cryptocurrency to another with the same hashing function can be explored
Nayak, K, et al.[16]	Analyzes Stubborn mining and its profitability	Combining mining attacks and network level attacks	crypto mining attack and network level attacks are combined to earn the miners more revenue by combining the attacks to form a complex strategy, to perform analytics with optimal parameters for the same strategy	To design a secure consensus protocol whose security is on rationality assumptions
Bai, Q. et al.[17]	Profitability of selfish mining	Markov chain to describe at tacker and honest miners	The minimum hash rate along with the minimum time taken to become profitable is derived	Rather than miners with small hash rate, miners with more hash rate can collaborate together to get more benefit. Hence a classification algorithm for the hash rate of miners can be devised.

Saad, M. et al.[18]	Defense strategy for selfish mining	In order to find the behavior of selfish mining, the block publishing height along with the transaction confirmation height	In order to Disincentivize the selfish miners, a network wide defense mechanism was utilized	By including the predictable confirmation height in the each transactions, the processing overhead and the fees overhead can be analyzed
Negy, K.A. et al.[19]	Profitability of selfish mining	New selfish mining known as intermittent selfish mining is developed	This strategy is more profitable than honest mining	Comparison between intermittent selfish mining and smart mining can be carried out
Sapirshtein, A. et al. [20]	Profitability of selfish mining	Model for profitability of selfish mining in the presence of communication delays	Algorithm that finds E-optimal policies for selfish miners and for the profitable attack, the fraction of resources is minimized.	The algorithm proposed by them can be used to reduce the profitability
Eyal, I. et al. [21]	The basic model of selfish mining	The blockchain selects the longest branch when a fork occurs	After the first DAA, the honest miners get attracted to the selfish mining pool along with the start mining on the head of the fork of selfish miners	A novel method to divert the honest miners from joining the selfish mining pool can be devised
Zhu, s. et al.[22]	Survey of Reward Distribution mechanisms in pool mining. Survey of Pool attack strategies and defense mechanisms have been examined	Pay per share mechanism, Pay per last N share mechanism, slush mechanism, geometric mechanism, double geometric Mechanism has been extensively studied	Existing reward distribution mechanisms has been studied. Summarization of the block withholding attacks with defense strategies has been done	Fair and secure practices in bitcoin mining pools with validation has yet to be found out
Zhang, S. et al.[23]	Game models are proposed to address the denial of service, selfish mining and majority attack. Economic trading and energy the block chain, pool allocation and reward allocation, also the power allocations also considerable issues in mining management.	Game theory models in reward allocation in block mining, energy trading is analyzed. Sequential game, repeated game, potential game, extensive form of game and non-cooperative form of game are various games used in all the papers surveyed	Reviewed and analyzed using game theory to deal with security and blockchain mining management	Game theoretical approach to incentive mechanism design can be devised
Francesco et al.[24]	Blockchain activities are monitored and the Ethereum log files are analyzed for anomalous behavior	Log files with time stamp of Ethereum Classic is analyzed for anomaly in time series	Variable auto encoder is used for anomaly detection	A bitcoin blockchain can be used for anomaly detection
Sudeep et al.[25]	Analyze the attack on blockchain based net works	Machine learning approach to make blockchain more resilient to attacks including majority attack and double spending	IDS that works on fraudulent transactions and network attacks in blockchain based energy applications	Quantum resilience and privacy issues has not been declared
J Niu et al.[26]	Determine the threshold of computational power for selfish mining profitability In Ethereum, the selfish mining profitability is controlled by the threshold of computational power.	Two-dimensional Markov process that models the selfish mining Ethereum. In order to determine the long term average mining rewards, the stationary distribution of Markov model was utilized	The threshold of computational power is lower than 25% as cited by Eyal and Sirer	The major limitation of selfish mining is controlled by the mining mechanism, When the mining mechanism is modified, selfish mining pool make major impacts its mining strategy to maximize its profit. This has to be solved.
Heilman, E.et al. [27]	Defense mechanism to selfish mining	Incentive compatible defense mechanism against selfish mining	The threshold power of mining is raised from 25% to 32% by unforgeable timestamps	Freshness of the next block is to examined
Jang J et al.[28]	Number of quantitative resources to profitable double spending attack is analyzed	Derivation of the probability distribution function of the attack success time is done	The less is the block confirmation number, minimum resource is needed for attack	Given the value of the transaction, the network can provide a service to inform the payee with the least block confirmation number that reduces the profit of double spending attack.
Kedziora, M. et al. [29]	Attack on the proof of work consensus of the blockchain with selfish mining strategy	Persistent mining algorithm in pursuit of a longer chain with a modified selfish extraction algorithm is used	Persistent mining algorithm works better with the hash rate of the selfish miners > 0.37	Malicious block extraction strategies can be explored in detail
Saad, M.et al.[30]	The attack surface of the blockchain has been analyzed	The attacks on the blockchain structure, attacks on the decentralized peer to peer system, at tacks on blockchain applications have been exhaustively studied	The attacks have been outlined. The counter measures are surveyed, major threats to blockchain and how one attack may facilitate the other attacks	The hash rate of the attackers plays a vital role and any machine learning or deep learning algorithm can be deployed for the same
Chicarino et al.[31]	Detection of selfish mining	Blockchain height deviates from a standard heighten alert is created	The probability of detection of selfish mining is 99.99%	The detection has false positive rate which can be resolved by machine learning methods

VI. Conclusion

In this paper we have given the blockchain, mining basics and an comprehensive survey on the selfish mining attack. We have taken 37 papers and made an exhaustive analysis of the deployment of machine learning, deep learning and reinforcement learning algorithms in various ways such as clustering of crypto addresses, classification of crypto addresses, revenue prediction, crypto currency price prediction and in the mitigation of selfish mining attacks in blockchain. We discussed the usage of bandit algorithms and it's research directions in the alleviation of selfish mining attacks. We hope that the survey will guide in the design of many selfish mining attack mitigation methods and will lead to more exploration, during selection of the next block of the main canonical blockchain, when a fork occurs.

References

[1] Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin. URL: https://bitcoin. org/bitcoin.pdf 4 (2008).

[2] Narayanan, Arvind, et al. "Bitcoin and cryptocurrency technologies." (2021).

[3] Henry, Ryan, Amir Herzberg, and Aniket Kate. "Blockchain access privacy: Challenges and directions." IEEE Security and Privacy 16.4 (2018): 38-45.

[4] Chohan, Usman W. "The double spending problem and cryptocurrencies." Available at SSRN 3090174 (2021).

[5] Nicolas, Kervins, et al. "Blockchain system defensive overview for double- spend and selfish mining attacks: A systematic approach." IEEE Access 9 (2020): 3838-3857.

[6] Simon, Jeyasheela Rakkini, and K. Geetha. "Block Mining reward prediction with Polynomial Regression, Long short-term memory, and Prophet API for Ethereum blockchain miners." ITM Web of Conferences. Vol. 37. EDP Sciences, 2021.

[7] http://xblock.pro/xblock-eth.html.

[8] Chang, Tao-Hung, and Davor Svetinovic. "Improving bitcoin ownership identification using transaction patterns analysis." IEEE Transactions on Systems, Man, and Cybernetics: Systems 50.1 (2018): 9-20.

[9] Rakkini MJ, and Geetha K. Deep learning classification of bitcoin miners and exploration of upper confidence bound algorithm with less regret for the selection of honest mining. Journal of Ambient Intelligence and Humanized Computing. 2021 Oct 24:1-7.

[10] Rakkini, Jeyasheela, and K. Geetha. "Stochastic Gradient Descent with Selfish Mining Attack Parameters on Dash Difficulty Adjustment Algorithm." Machine Vision and Augmented Intelligence—Theory and Applications. Springer, Singapore, 2021. 589-597.

[11] Davidson, Michael, and Tyler Diamond. "On the profitability of selfish mining against multiple difficulty adjustment algorithms." Cryptology ePrint Archive (2020).

[12] Eijkel, D., and FehnkSaad, M., Njilla, L., Kamhoua, C., and Mohaisen, (2019, February). Countering selfish mining in blockchains. In 2019 International Conference on Computing, Networking, and Communications (ICNC) (pp. 360-364). IEEE.er, A. (2019, October).

[13] Gober, J.A., 2018. The Dynamics of a" Selfish Mining" Infested Bitcoin Network: How the Presence of Adversaries Can Alter the Profitability Framework of Bitcoin Mining (Doctoral dissertation).

[14] Zhang, R., and Preneel, B. (2017, February). Publish or perish: A backwards- compatible defense against selfish mining in bitcoin. In Cryptographers' Track at the RSA Conference (pp. 277-292). Springer, Cham.

[15] Grunspan, Cyril, and Ricardo Pérez-Marco. "On profitability of selfish mining." arXiv preprint arXiv:1805.08281 (2018).

[16] Nayak, K., Kumar, S., Miller, A., and Shi, E. (2016, March). Stubborn Mining: Generalizing selfish mining and combining with an eclipse attack. In 2016 IEEE European Symposium on Security and Privacy (EuroSandP) (pp. 305-320). IEEE.

[17] Bai, Q., Zhou, X., Wang, X., Xu, Y., Wang, X., and Kong, Q. (2019, May). A deep dive into blockchain selfish mining. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[18] Saad, M., Njilla, L., Kamhoua, C., and Mohaisen, A. (2019, February). Countering selfish mining in blockchains. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp.360-364). IEEE.

[19] Negy, K. A., Rizun, P. R., and Sirer, E. G. (2020, February). Selfish Mining Re- Examined. In International Conference on Financial Cryptography and Data Security (pp. 61-78). Springer, Cham.

[20] Sapirshtein, A., Sompolinsky, Y., and Zohar, A. (2016, February). Optimal selfish mining strategies in bitcoin. In International Conference on Financial Cryptography and Data Security (pp. 515-532). Springer, Berlin, Heidelberg.

[21] Eyal, I., and Sirer, E. G. (2014, March). Majority is not enough: Bitcoin mining is vulnerable. In International conference on financial cryptography and data security (pp. 436- 454). Springer, Berlin, Heidelberg.

[22] Zhu, S., Li, W., Li, H., Hu, C., and Cai, Z. (2018). A survey: Reward distribution mechanisms and withholding attacks in Bitcoin pool mining. Mathematical Foundations of Computing, 1(4), 393.

[23] Zhang, S., Zhang, K., and Kemme, B. (2020, May). A simulation-based analysis of multi-player selfish mining. in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-5). IEEE.

[24] Scicchitano, F., Liguori, A., Guarascio, M., Ritacco, E., and Manco, G. (2020). A Deep Learning Approach for Detecting Security Attacks on Blockchain. In ITASEC (pp. 212-222).

[25] Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P. K., and Hong, W. C. (2019). Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. IEEE Access, 8, 474 488.

[26] Feng, Chen, and Jianyu Niu. "Selfish mining in ethereum." In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 1306-1316. IEEE, 2019.

[27] Heilman, E. (2014, March). One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. In International Conference on Financial Cryptography and Data Security (pp. 161-162). Springer, Berlin, Heidelberg.

[28] Jang, J., and Lee, H. N. (2020). Profitable double-spending attacks. Applied Sciences, 10(23), 8477.

[29] Kedziora, M., Kozlowski, P., Szczepanik, M., and Jo´z´wiak, P. (2019, September). Analysis of blockchain selfish mining attacks. In International Conference on Information Systems Architecture and Technology (pp. 231-240). Springer, Cham.

[30] Saad, Muhammad, et al. "Overview of attack surfaces in blockchain." Blockchain for distributed systems security (2019): 51-66.

[31] Chicarino, Vanessa, et al. "On the detection of selfish mining and stalker attacks in blockchain networks." Annals of Telecommunications 75.3 (2020): 143-152.

[32] Wang, Taotao, Soung Chang Liew, and Shengli Zhang. "When blockchain meets AI: Optimal mining strategy achieved by machine learning." International Journal of Intelligent Systems 36.5 (2021): 2183-2207.

[33] Hou, Charlie, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramer, Giulia Fanti, and Ari Juels. "SquirRL: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning." arXiv preprint arXiv:1912.01798 (2019).

[34] Yang, Guoyu, Yilei Wang, Zhaojie Wang, Youliang Tian, Xiaomei Yu, and Shouzhe Li. "IPBSM: An optimal bribery selfish mining in the presence of intelligent and pure attackers." International Journal of Intelligent Systems 35, no. 11 (2020): 1735-1748.

[35] Liu, Chi Harold, Qiuxia Lin, and Shilin Wen. "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning." IEEE Transactions on Industrial Informatics 15.6 (2018): 3516- 3526.

[36] Lu, Cong, et al. "Challenges and Opportunities in Offline Reinforcement Learning from Visual Observations." arXiv preprint arXiv:2206.04779 (2022).

[37] Shi, Laixi, et al. "Pessimistic q-learning for offline reinforcement learning: Towards optimal sample complexity." arXiv preprint arXiv:2202.13890 (2022).