INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 4th Sept 2020. Link :http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-09

Title: **SURVEY ON MINING ATTACKS ON BLOCKCHAIN**

Volume 09, Issue 09, Pages: 120-126

Paper Authors

D SWAPNA, A MADHURI, T SRI LAKSHMI, S SINDHURA.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SURVEY ON MINING ATTACKS ON BLOCKCHAIN

D SWAPNA, A MADHURI, T SRI LAKSHMI, S SINDHURA.
[1-3]Assistant professor, Department of Computer Science and Engineering,
Prasad V Potluri Siddhartha Institute of Technology (Autonomous), Vijayawada.A.P,India,
[4]Assistant Professor, Department Of Computer Science and Engineering, KoneruLakshmaiah Education Foundation, Vaddeswaram, AP, India

Abstract:

The blockchain technology came to light in 2008 as a decentralised peer to peer network structure, with the ability to ensure security for transactions made on bitcoin cryptocurrency, without the need of any central server to validate transactions. Although it started with the advent of cryptocurrencies,it is being used in several areas to develop different projects like electronic voting, supply chain managememt,banking .With its vast usage ,issues arise with potential attacks on mining pools of blockchain. This paper classifies the various mining pool attacks and their existing countermeasures.

Introduction

Blockchain tis the key innovation launched by introducing a cryptocurrency called bitcoin which was formulated in 2008 by Satoshi[1]. Blockchain technology imparts a mechanism to ensure integrity ,authenticity, immutability, auditing and irrevocability to maintain security for e-transactions. Blockchain technology eliminates necessity of third parties as all records are distributed among all participants present over the Blockchain network.

Even with many in-built features ensuring security of blockchain, current reports have emphasized security risks linked with blockchain technology[2]-[6].For example, on July 2016 an anonymous attacker ditched $50 million USD form Decentralised Autonomous Organization that works on Ehereum blockchain based smart contracts. From Bitfinex which is a Bangkok based bitcoin exchange platform $72 million worth bitcoins were stolen[7]. Distributed denial-of-surface(DDoS) attack on Bitfinex resulted in temporary suspension of exchange platform.Often many exchange platform etherurm and bitcoin experienced DNS and DDoS Attacks which resulted in blocking the availability of services to users.

For example, Attacks will cause decline of the cryptocurrencies,fall of mining incentives and even closing of cryptocurrency exchange platforms.[8] In 2017 Bitcoin Memory pools faced spam or dust transactions to initiate delay in transaction validation,and to raise Bitcoin mining rewards[9].Bitcoins faced a payment block of $700 million USD due to delay in transactions[10].The objective of such attacks is to make users to migrate to other cryptocurrency platforms with better processing times.

With rapid development of applications using blockchain, the fundamental factor is to ensure security for data residing on blockchain. At present,attackers are conducting several attacks on blockchain using the features of blockchain,which causes data on blockchain to face several threats. The attacks on Blockchain network causes unnatural or improper access to data on blockchain, which threaten the blockchain data availability, Internet protocol(IP) address and bitcoin address can be associated with each other. Tracking of users, actualidentity,coherence among addresses can be done by attackers[11,12].Transactions made on blockchain expose relationships between the addresses to attackers because of its openness privacy of users is exposed[13]. Data on Blockchain gets tampered if Consensus mechanism of blockchain is attacked by attacker. Selfish Mining attacks are also possible in blockchain [14,15,16].Integrity of data on blockchain will be ruined because of these attacks. Usage of same cryptocurrency in numerous transactions by trader is known as Double spending attack. Miner decides to abandon the legal block that has been found because of this mining pool loses all incentives related to that block[17].

The paper is organised as follows Section 1 describes what a mining pool is. Section 2 classifies and summarizes various mining pool attacks Section 3 Surveys the various existing countermeasures of mining pool attacks

What is a mining pool

Miners community is the backbone behind working of a blockchain. New blocks are added to blockchain by miners by fixing the cryptographed puzzles which indeed needs a greater strength for computation. If miners successfully adds a block, they are rewarded with 12.5 BTC.

There was a certain limit on the numbers of bitcoins i.e., only twenty one million bitcoins will be generated. Bitcoin creator Satoshi anticipated that if entry of miners increase progressively then bitcoin price would rise exponentially, to such an extent that entire bitcoins can be mined in two or three years

Presently, it could be fiasco for all bitcoins, in light of the fact that like every single financial item, the estimation of bitcoin lies in market interest. On the off chance that the stockpile of bitcoins out of nowhere expands, at that point that would diminish the interest, which would thus hurt its worth.

A system for adjusting difficulty has been implemented by Satoshi makes the bitcoin network more sustainable to restrict bitcoin supply. Difficulty adjustment means as count of mined bitcoins raises the hardness attributed to cryptographic puzzles raise exponentially.

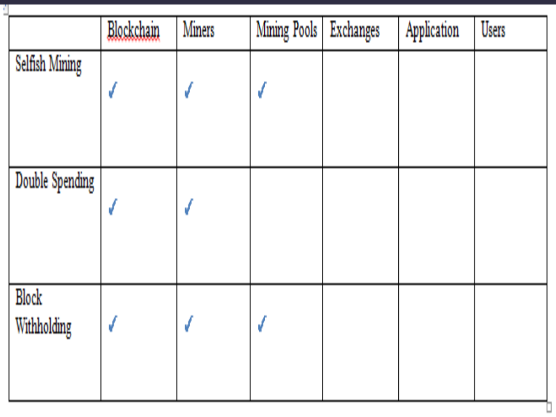
Miners soon realized that mining can’t be done efficiently by themselves, process is getting complex and expensive as bitcoins are being mined. So Miners to decided to pool their assets that is computing power together and form groups to perform bicoin mining efficiently. Such type of pools and miners forming a group to perform mining together called “mining pools”.

Cause of Mining Pool Attacks

51% attack arises when the 51% of the system's hashrate is under control of a single mining pool or any other individual. 51% attacks enacts the system to a number of attacks such as

- Selfish mining,
- Double Spending,
- Block with holding attack

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org



	Blockchain	Miners	Mining Pools	Exchanges	Application	Users
Selfish Mining	✓	✓	✓			
Double Spending	✓	✓				
Block Withholding	✓	✓	✓			

Table 1: Attacks effecting the mechanism of blockchain

Causes for 51%attack

1) A mining pool turns out to be too enormous
2) Having boundless capital

Selfish mining:

Eyal and Sirer[18] introduced selfish mining attack in 2013. Bitcoin Proof of Work incentives is not compatible for incentives if selfish mining has occurred, due to which attackers receive higher incentives. Wasting mining power of honest miners on unneeded computations is the preliminary concept of selfish mining attack. Without directly disclosing blocks to blockchain network attacker keeps it confidential to create a fork. Hence, the intention of attacker is to make blocks mined by genuine miners orphan.

Honestly mined blocks are represented with purple colour, blocks mined by selfish miners are represented with black colour and blocks already present in valid blockchain are represented with yellow colour. Presence of new blocks are represented with shadowed boxes. New block found by selfish miners are represented with black shadowed box and purple shadowed box represents new block found by honest miner. Case one in Fig:1depicts a blockchain fork and a block identified by selfish miner. Then immediately blockchain fork ends and reward of two blocks is gained .Case 2 depicts that when there is a blockchain fork and new block mined by honest miners is connected to selfish miner's blockchain, then both honest and selfish miners receive their respective revenue for each block.Case 3 depicts that new blocks mined by honest miner are connected to blockchain of honest miners then incentive of two blocks is received by honest miner.

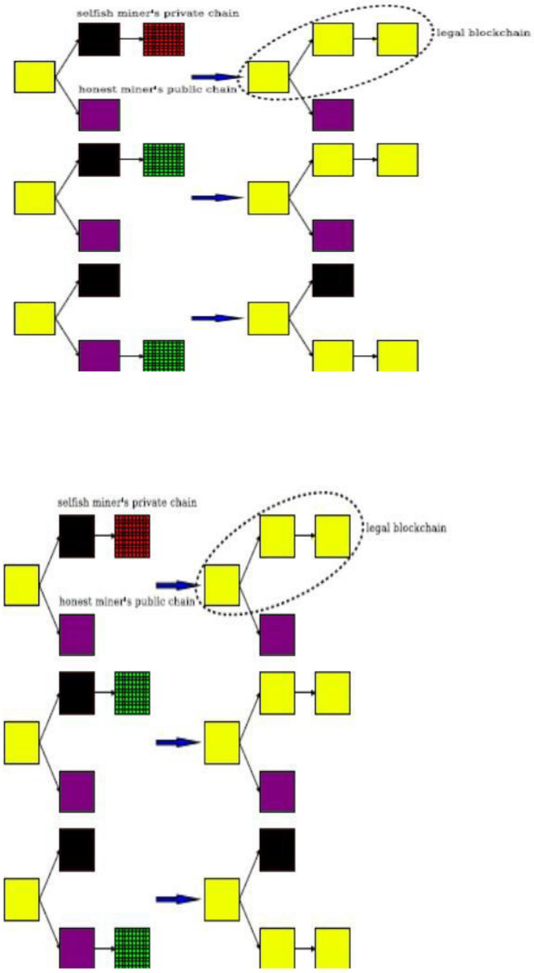

selfish miner's private chain
legal blockchain
honest miner's public chain
selfish miner's private chain
legal blockchain
honest miner's public chain

Fig: Selfiish Mining

Double Spending

The attack performed by malicious users to betray the system is known as double spending. Duplicates of Unspent Transaction Output(UTXO) of a cryptocurrency is generated an it is used as an input for many transactions. These type of attacks are defended by system by trusting miners to approve the validity of crypto currencies used as transaction input.

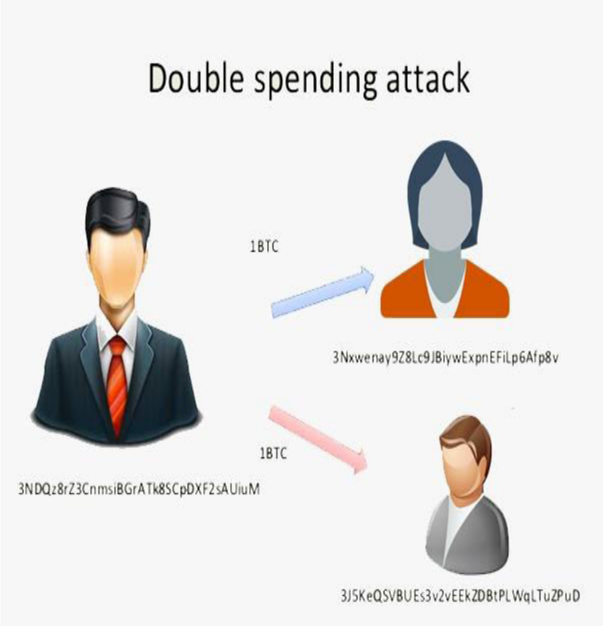

Double spending attack
1BTC
3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v
1BTC
3NDQz8rZ3CnmsiBGrATk8SCpDXF2sAUiuM
3J5KeQSVBUEs3v2vEEkZDBtPLWqLTuZPuD

Fig:Double Spending Attack

Under such circumstances, the blockchain industry needs to understand the double-spending problem in Bitcoin profoundly.

Problem of double-spending cannot be neglected in the world of blockchain.In May 2018 Bitcoin Gold Network(BTG) suffered a double spending attack by a malicious miner,whosecryptocurrency is most valuable in world ranked 26.Miner acquires momentary control of blockchain if they gain 51% of entire network's hashpower. Attackers stole over 389,200 BTG and deposited them on crypto exchanges

Block withholding attack

Block withholding is yet another type of selfish mining. ASIC's are used by miners in network of bicoin to conduct mining.Mining blocks is an extremely simple job for those miners. They mine a block but will not expose to the network. Rather than announcing to the blockchain network and collecting the reward miner's keep the block a secret as well as mine in next block in addition to that.

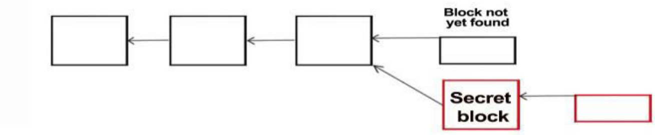


Fig: Block Withholding attack

The "secret blocks" are actually those which miners had mined and withheld from the remaining blockchain network. Whenever miners do look for another block, miners are able to expose the 2 blocks to the blockchain network.

Exactly why it's known as "selfish", is actually since miners are moving from the reality concept of "equal chance of all" this mining means. Everybody should have a good shake at giving mining as well as finding out the own blocks of theirs. In addition, this could additionally result in community monopolization.

Effects of these attacks

Prevention

Ruffing et al[19] created a contract on blockchain that permits beneficiaries to get refunds asynchronously & enforce fine on attackers involved in double-spending.Eleftherios et al recommended an interesting Byzantine consensus mechanism based on byzantine fault tolerance which short-conclude trading period by 15 to 20 seconds as well as utilized mutual signatures to generate irreversible transactions. George et al[20] unveiled a cryptocurrency named RSCoin,where the central bank provides total command with the coin source to counteract problem of double-spending.

In order to counter block withholding attacks Schrijve et al. [21] unveiled a reward system that is suitable for incentives and intimidates wicked miners from undertaking withholding attacksfrom the precise pool of miners.Rosenfeld[22] unveiled Honeypot method for bribing crooked miners and hence miners holding legitimate fixes can be caught.Sakurai and Bag [23] proposedadded rewards for locating a legitimate option for a block to be able to avoid mining conspiracy.Contemporaneous to their previous research Bag et al[24] unveiled a brand-new plan that gropes pool of miners from present goal to complicate their power to differentiate in between a full PoW and partial PoW.Their recommended solution additionally secures the pooldriver to prettyspread incentive to the successful miner.

To decrease overall benefits of other group at the time of mining miner's attack one another. Yang et al. [25] unveiled a game method among two miners to enhance profit of miners. If a trustworthy miner employs a fixing plan, can unnaturally reward a selfish miner within 0 to i=2-p (p is power of computing and I is increase in profit), disregarding the plan of a selfish miner.

Miller et al. [26] recommended an alliance mechanism for mining pools where the mining pool members didn't believe in one another, but they reveal their contribution by submitting a confidential certificate. Shi [27] altered the mechanism of consensus of Bitcoin, where specific guidelines are followed to make certain the steady gain of Bitcoin. This method is able to boost up distribution and minimize chance of 51 % attack. Gervais et al. [28] interpreted different arguments of POW. They created probably the better preventive measures for selfish mining and double-spending.

Conclusion

With the improvement of blockchain, its usage is increasingly considerable, but various security threats of blockchain itself are slowly revealed. In this article, we surveyed the mining pool attacks of Blockchain Technology. We classified and summarized various mining pool attacks which are a threat to the mechanism of blockchain. After classifying these attacks we had surveyed the existing counter measures for double spending, selfish mining and block withholding attacks. In our future research we extend to develop a countermeasure for 51% attacks which is the main reason behind mining pool attacks

Reference

1 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Nakamoto Institute. 2008.

2 E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A.de A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," Security and Communication Networks, vol. 2018, pp. 9 675 050:1–9 675 050:27, 2018. [Online].

Available:https://doi.org/10.1155/2018/9675050

[3] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," CoRR, vol. abs/1802.06993, 2018.[Online].Available: http://arxiv.org/abs/1802.06993

[4] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges." IJ Network Security, vol. 19, no. 5, pp. 653–659, 2017.[5] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attack so nether eumsmart contracts sok," in Proceedings of the 6thInternational Conference on Principles of Security and Trust –Volume 10204, 2017, pp. 164–186. [Online]. Available: https://doi.org/10.1007/978-3-662-54455-6_8

[6] M. C. K. Khalilov and A. Levi, "A survey on anonymity andprivacy in bitcoin-like digital cash systems," IEEE Communications Surveys and Tutorials, vol. 20, no. 3, pp. 2543–2585, 2018. [Online].Available: https://doi.org/10.1109/COMST.2018.2818623

[7]C. Baldwin, "Bitcoin worth 72 million stolen from bitfinex exchange in Hong Kong," http://reut.rs/2gc7iQ9, Aug 2016.

[8]M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin:Routing attacks on cryptocurrencies," in Proceedings of the 38thIEEE Symposium on Security and Privacy (Oakland). San Jose,CA: IEEE, May 2017, pp. 375–392. [Online]. Available: https: //doi.org/10.1109/SP.2017.29

[9] M. Saad, M. T. Thai, and A. Mohaisen, "POSTER: deterringddos attacks on blockchain-based cryptocurrencies through mempool optimization," in Proceedings of Asia Conference on Computer and Communications Security, ASIACCS, Incheon, Republic of Korea, Jun2018, pp. 809–811. [Online]. Available: https://goo.gl/4kgiCM

[10] F. Memoria, "700 million stuck in 115,000 unconfirmed bitcoin transactions," Nov 2017. [Online]. Available: https://www.cryptocoinsnews.com/700-million-stuck-115000-unconfirmed-bitcoin-transactions/

[11]P. Koshy, D. Koshy, P. McDaniel, An analysis of anonymity in bitcoin usingp2p network trac. In Proc. of Financial Cryptography and Data Security,2014, pp. 469-485.

[12] A. Biryukov, D. Khovratovich, I. Pustogarov, Deanonymisation of clientsin bitcoin p2p network. In: Proc. of Computer and Communications Security,2014, pp. 15-29.

[13]F. Reid, M. Harrigan, An analysis of anonymity in the bitcoin system, In:Proc. of IEEE Third International Conference on Privacy, Security, Risk and Trust, 2012, pp. 1318-1326.

[14] L. Bahack, Theoretical bitcoin attacks with less than half of the computational power, Computer Science, 2013, doi:http://arxiv.org/abs/1312.7013v1.

[15] S. Bag, S. Ruj, K. Sakurai, Bitcoin block withholding attack: Analysis and mitigation, IEEE Transactions on Information Forensics & Security, 12(8) (2017):1967-1978.

[16] I. Eyal and E. G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, In: Proc. of International conference on _nancial cryptography and data security, 2014, pp. 436-454.

[17]Wu, Di & Liu, Xiangdong & Yan,

Xiangbin & Peng, Rui& Li, Gang. (2019). Equilibrium analysis of bitcoin block withholding attack: A generalized model. Reliability Engineering [?]System Safety. 10.1016/j.ress.2018.12.026.

[18]https://medium.com/@deependrasg/what-is-double-spending-problem-in-blockchain-how-bitcoin-solve-this-problem-9f9f1c237db0

[19] T. Ru_ng, A. Kate, D. Schroder, Liar, liar, coins on _re: Penalizing equivocation by loss of bitcoins, In: Proc. of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 219-230.

[20] G. Danezis, S. Meiklejohn, Centrally banked cryptocurrencies, 2016, http://www0.cs.ucl.ac.uk/sta_/S.Meiklejohn/_les/ndss16slides.pdf).

[21] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, “Incentivecompatibility of bitcoin mining pool reward functions,” in 20thInternational Conference on Financial Cryptography and DataSecurity FC, Christ Church, Barbados, Feb 2016, pp. 477–498.[Online]. Available: https://doi.org/10.1007/978-3-662-54970-4_28

[22] M. Rosenfeld, “Analysis of bitcoin pooled mining reward systems,”CoRR, 2011. [Online]. Available: http://arxiv.org/abs/1112.4980

[23] S. Bag and K. Sakurai, “Yet another note on block withholding attack on bitcoin mining pools,” in 19th International Conference on Information Security ISC, Honolulu, HI, USA, Sep 2016, pp. 167–180.
[Online]. Available: https://doi.org/10.1007/978-3-319-45871-7_11

[24] S. Bag, S. Ruj, and K. Sakurai, “Bitcoin block withholding attack:Analysis and mitigation,” IEEE Trans. Information Forensics and Security, vol. 12, no. 8, pp. 1967–1978, 2017. [Online]. Available: https://doi.org/10.1109/TIFS.2016.2623588

[25]A. Juels, A. Kosba, E. Shi, The ring of gyges: Investigating the future of criminal smart contracts, In: Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 283-295.

[26][83] A. Miller, A. Kosba, J. Katz, E. Shi, Non outsourceable scratch-o_ puzzles to discourage bitcoin mining coalitions, In: Proc. of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 680-691.

[27] N. Shi, A new proof-of-work mechanism for bitcoin, Financial Innovation, 2(1) (2016) 31.

[28]A. Gervais, G. O. Karame, K.Wust, V. Glykantzis, H. Ritzdorf , S. Capkun, On the security and performance of proof of work blockchains. In: Proc. Of Conference on Computer and Communications Security, 2016, pp. 3-16. https://github.com/i13-msrg/vibes/blob/master/docs/Master_Thesis_VIBES.pdf