UNIVERSITI PUTRA MALAYSIA

Implementing of Forking After Withholding FAW Attack on Bitcoin System

AHMED MOHAMMED A. ALAHMADI

FSKTM 2018 40

Implementing of Forking After Withholding FAW Attack on Bitcoin System

By

AHMED MOHAMMED A. ALAHMADI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Information Security

JULY 2018

DEDICATIONS

To the amiability of difficult days and the moon of dark nights . . . my precious mother.

To my great father.

To each of who has taught me or gave me advice . . . teachers.

Dedicate this work . . .

ABSTRACT

Implementing of Forking After Withholding FAW Attack on Bitcoin System

Nowadays many applications have employed the blockchain technology from sample cryptocurrency to smart contracts applications. Bitcoin is one of the cryptocurrency application and digital payment system. It is considered as the first decentralized digital currency system. It was invented by unidentified person or group under the name of Satoshi Nakamoto in 2009 (Nakamoto, 2008). The most three features should be achieved by Bitcoin are decentralized, users anonymity, and consensus. In order to achieve these vital features the Bitcoin system should be provably secure against the attacks. Many attacks have been proposed to change unfairly the reward system of the mining pool and allow the malicious miners to earn undue wage. Selfish Attack, Block Withholding (BWH) Attack and Forking After Withholding (FAW) Attack are three attacks which abusing the reward system and letting the infiltration miners to receive un unearned profits and as a sequence this will affect the decentralized feature of the Bitcoin system. Some studies proposed a solution for Selfish Attack and Block Withholding attack such (Eyal and Sirer, 2014b) and (Bag et al., 2017). FAW attack is first introduced by (Kwon et al., 2017) where this attack combines two attacks: Selfish and BWH attacks. In order to come up with a solution for FAW attack (Kwon et al., 2017) propose partial countermeasures for preventing their FAW attack. However, their solution is neither perfect nor practical. Therefore this study addresses this attack and analyzes its strategy then come up with a prevention solution. The result of this study shows that our prevention solution is practical and more efficient.

ACKNOWLEDGMENTS

First and foremost, praise be to Allah through whose mercy (and favors) all good things are accomplished. ("My Lord, increase me in knowledge." . Surat Taha 20:114).

I would like to express the deepest appreciate and sincerest gratitude to my supervisor, Prof. Dr. Zuriati Ahmad Zukarnain , for her patience and truthful guidance through all the steps of the dissertation. I attribute the level of my Master degree to her encouragement and effort she spent for helping me accomplishing this work.

I thank and appreciate the valuable effort of my lecturers at Faculty of Computer Science and Information Technology (FSKTM), Universiti Putra Malaysia (UPM), Malaysia.

Finally, I owe many thanks to my parents for their dedication, help, and encouragement in those critical moments along this journey. I am deeply indebted to them for their unconditional support and sacrifice for so many years. Words are not enough to express my gratitude.

This dissertation was submitted to the Information Security Department, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of **Master of Information Security**.

Zuriati Ahmad Zukarnain, PhD
Prof. Dr
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia

Date: July 5, 2018

DECLARATION

I declare that the report is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

(Signature)

Ahmed M. A. AlAhmadi

Date: July 5, 2018

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BWH	Block Withholding Attack
BTC	Bitcoin
FAW	Forking After Withholding Attack
FPoW	Full Proof-of-Work
PPoW	Partial Proof-of-Work
PoW	Poof-of-Work

CHAPTER 1

INTRODUCTION

This chapter introduces the overview of the dissertation and explains the motivation for this work. Then it presents the problem statement, dissertation objectives and dissertation scope. At the end of this chapter dissertation report structure is provided.

1.1 Overview and Motivation

Blockchain technology plays a vital rule in the implementation of many application such as Bitcoin system (Narayanan et al., 2016). Bitcoin system attracts a lot of attention where the system can provide the users with decentralized payment system which does not depend on third party to manipulate and control the financial transactions. The security of Bitcoin system is very essential prospective. There are many attacks and vulnerabilities which threats the consensus and security of this system such as Double spending or Race attack, Finney attack, Brute force attack, Vector 76 or one-confirmation attack, ¿ 50% hashpower or Goldfinger, Block discarding or Selfish mining, Block withholding BWH attack, and fork after withholding (FAW) attack. Almost of them have been countermeasured. Unfortunately, Fork After Withholding FAW attack still open challenge. FAW attack was proposed by (Kwon et al., 2017) which originally combines two attacks (Selfish attack and Block Withholding BWH attack). Kwon et al. (2017) also present some countermeasures for their attack. One of these solutions is come up with a new reward system. However their proposed solution are not practical. As a sequence FAW attack is still an open challenge. Therefor we motivated to conduct this study to address FAW attack and come up with a prevention solution without enforcing to change within the Bitcoin protocol itself which is good to maintain the security of the Bitcoin system.

1.2 Problem Statement

The abusing of the forking mechanism leads to appear a type of attack called Selfish attack which proposed by (Eyal and Sirer, 2014b). Selfish attack allows the infiltration miner to generate intentional forks in order to receive reward more than their fair profit. This attack can have significant consequences for Bitcoin: Rational miners will prefer to join the selfish miners, and the infiltration group will increase in size until it becomes a majority. At this point, the decentralized feature of the Bitcoin will be affected (Eyal and Sirer, 2014b) and (Eyal and Sirer, 2014a). Another attack called Block Withholding BWH (Rosenfeld, 2011) which also let the malicious miner to earn undeserved wage by submitting Partial Proof-of-Works (PPoWs) instead of Full Proof-of-Works (FPoWs) pretending contribute work. By employing the strategy of these two attack Selfish Mining and BWH attacks (Kwon et al., 2017) propose a novel attack called a Fork After Withholding (FAW) attack (this attack which is always profitable (unlike selfish mining) regardless of the attackers network capability and computational power. The FAW attack allows the malicious miner (attacker) to earn undue wage four times more than Block Withholding (BWH) attack makes. In order to come up with a solution for this attack (Kwon et al., 2017) propose partial countermeasures for preventing FAW attack which combines both Selfish and Block Withholding attacks. They come up with a new reward system using a bonus system where the miner who submits FPoWs will get more reward than who submits PPoWs. However their high reward variance system makes miners hesitate to join the mining pool. Therefore, their solution is not piratical and the FAW attack mitigation is still an open challenge.

1.3 Objectives

The objective of this dissertation is to propose a tool for achieving the following objectives:

i. To propose a model for Forking After Withholding (FAW) attack on Bitcoin system and implement it.

ii. To propose a prevention solution which resists the Forking After Withholding (FAW) attack over Bitcoin.

iii. To evaluate the prevention solution to insure that the blockchain can detect the Forking After Withholding (FAW) attacker and prevent the attack.

1.4 Scope

The dissertation scope is shown in figure 1.1. We notice that this dissertation will concentrate on FAW attack which threats the security of the blocks of the Bitcoin system on the blockchain. This dissertation address this attack in order to prevent the Bitcoin miners and users form abusing or lost their reward and investments. In addition, it is important to notify that the dissertation will cover two other attacks namely Selfish Mining attack and Block Withholding BWH attack because FAW attack combines of these two attacks strategies together.

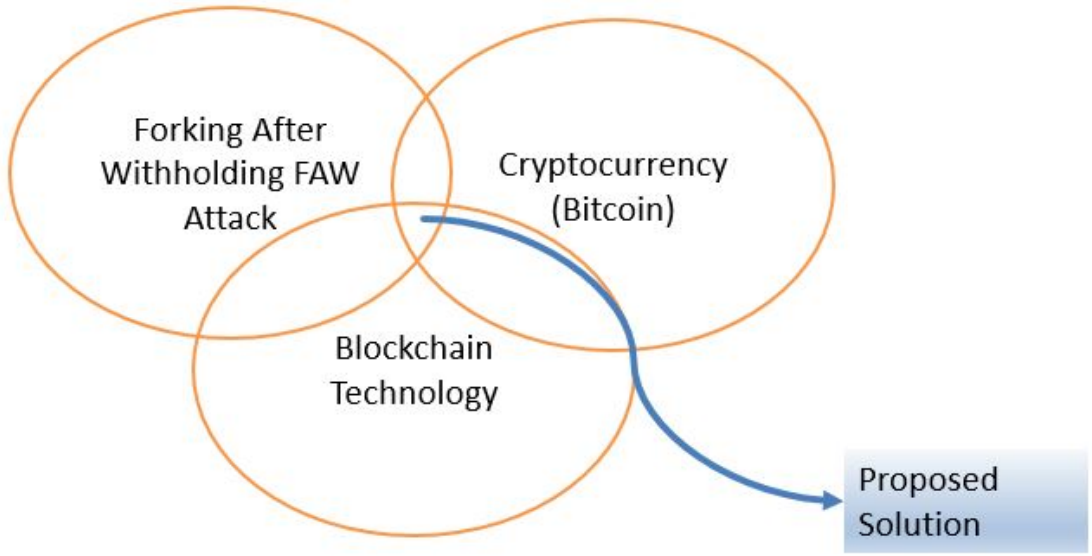

Figure 1.1: Scope of Dissertation

1.5 Organization of the Dissertation

This dissertation includes six chapters. Chapter 1 is an Introduction. Chapter 2 presents the literature review by discussing the Blockchain Technology and its application on Bitcoin and concentrates on the Bitcoin's attack called Forking After Withholding (FAW) attack . The dissertation methodology is explained in chapter 3. Chapter 4 elaborates the modeling of the FAW attack and implementation of the proposed prevention solution. Chapter 5 presents the results and discussions. Finally the conclusion and some suggestions for future work are covered in chapter 6.

REFERENCES

Babaioff, M., Dobzinski, S., Oren, S. and Zohar, A. 2012. On bitcoin and red balloons. In *Proceedings of the 13th ACM conference on electronic commerce*, 56–73. ACM.

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

Bahack, L. 2013. Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft). *arXiv preprint arXiv:1312.7013* .

Bamert, T., Decker, C., Elsen, L., Wattenhofer, R. and Welten, S. 2013. Have a snack, pay with Bitcoins. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, 1–5. IEEE.

Barber, S., Boyen, X., Shi, E. and Uzun, E. 2012. Bitter to betterhow to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security*, 399–414. Springer.

Bastiaan, M. 2015. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. In *Availab le at http://referaat. cs. utwente. nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin. pdf* .

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. and Felten, E. W. 2015. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *Security and Privacy (SP), 2015 IEEE Symposium on*, 104–121. IEEE.

Camacho, P., Lerner, S. D., Erhardt, M., Heilman, E., Alshenibr, L., Baldimtsi, F., Scafuro, A., Goldberg, S., Kokoris-Kogias, E., Jovanovic, P. et al. 2016, Decor+ LAMI: A scalable blockchain protocol, Tech. rep.

Clark, J. B. A. M. J., Edward, A. N. J. A. K. and Felten, W. 2015. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *url: https://eprint. iacr. org/2015/261. pdf* .

Conti, M., Kumar, S., Lal, C. and Ruj, S. 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials* .

Courtois, N. T. and Bahack, L. 2014. On subversive miner strategies and block withholding attack in bitcoin digital currency. *arXiv preprint arXiv:1402.1718* .

Daian, I. E. P., Sirer, E. G. and Juels, A. 2017. Piecework: Generalized outsourcing control for proofs of work. In *BITCOIN Workshop*.

Douceur, J. R. 2002. The sybil attack. In *International workshop on peer-to-peer systems*, 251–260. Springer.

Duong, T., Chepurnoy, A., Fan, L. and Zhou, H.-S. 2018. TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, 1–13. ACM.

Eastlake 3rd, D. and Hansen, T. 2011, US secure hash algorithms (SHA and SHA-based HMAC and HKDF), Tech. rep.

Eyal, I. 2015. The miner's dilemma. In *Security and Privacy (SP), 2015 IEEE Symposium on*, 89–103. IEEE.

Eyal, I. and Sirer, E. G. 2014a. How to disincentivize large bitcoin mining pools. *Blog post: http://hackingdistributed. com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools* .

Eyal, I. and Sirer, E. G. 2014b, In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, , vol. 8437, 436–454, 436–454.

Eyal, I. and Sirer, E. G. 2014c. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM* 61 (7): 95–102.

Finney, H. 2011, Best practice for fast transaction acceptance-how high is the risk.

Heilman, E. 2014. One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. In *International Conference on Financial Cryptography and Data Security*, 161–162. Springer.

Heusser, J. 2013, SAT solving-An alternative to brute force bitcoin mining, Tech. rep., Technical Report. https://jheusser. github. io/2013/02/03/satcoin. html.

Karame, G. O., Androulaki, E. and Capkun, S. 2012. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, 906–917. ACM.

Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A. and Čapkun, S. 2015. Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC)* 18 (1): 2.

Kraft, D. 2016. Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications* 9 (2): 397–413.

Kroll, J. A., Davey, I. C. and Felten, E. W. 2013. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS*, 11.

Kwon, Y., Kim, D., Son, Y., Vasserman, E. and Kim, Y. 2017. Be Selfish and Avoid Dilemmas. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17*, 195–209. New York, New York, USA: ACM Press.

Miller, A. 2013, Feather-forks: enforcing a blacklist with sub-50% hash power.

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

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Nayak, K., Kumar, S., Miller, A. and Shi, E. 2016. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*, 305–320. IEEE.

Rosenfeld, M. 2011. Analysis of bitcoin pooled mining reward systems. *arXiv preprint arXiv:1112.4980* .

Sapirshtein, A., Sompolinsky, Y. and Zohar, A. 2016. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, 515–532. Springer.

Solat, S. and Potop-Butucaru, M. 2017. Brief announcement: Zeroblock: Timestamp-free prevention of block-withholding attack in bitcoin. In *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, 356–360. Springer.

Szabo, N. 1997. Formalizing and securing relationships on public networks. *First Monday* 2 (9).

Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C. A., Kwiat, K. A. and Njilla, L. 2017. Security implications of blockchain cloud with analysis of block withholding attack. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 458–467. IEEE Press.

Zhang, R. and Preneel, B. 2017. Publish or perish: A backward-compatible defense against selfish mining in bitcoin. In *Cryptographers Track at the RSA Conference*, 277–292. Springer.