Bitcoin Block Withholding Attack : Analiza in ublažitev napada

Anej Budihna,Luka Golinar, Matjaz Glumac

13. maj 2017

Povzetek

Avtorji se posvetijo dvema problemoma: prvi je študija različice napada imenovanega "bločno prikrivanje"(angl. block withholding attack - BWA) v Bitcoinih in drugi je priporočilo rešitev za preprečitev vseh obstoječih vrst BWA napadov. Predstavijo analize strategij sebičnega Bitcoin rudarja, ki v potuhi z neko skupino rudarjev poskuša napadati neko drugo skupino in pri tem dobi določeno nagrado, ker je prisostvoval pri napadu na drugo skupino. Tak napad so avtorji poimenovali šponzorirani napad z bločnim prikrivanjem". Poleg tega predstavijo podrobno kvantitivno analizo dobičkonosnosti, ki jo lahko sebični rudar pridobi s tem, ko rudar uporablja omenjen napad v različnih primerih. V članku avtorji dokažejo, da ob določenih pogojih lahko napadalec optimalno poveča svoj prihodek z uporabo nekaterih strategij in s pametnim izkoriščanjem svojih računalniških virov. Pokažejo tudi, da lahko napadalec uporabi to strategijo za napad na obe skupini, da bi pri tem lahko dosegel višjo dobičkonosnost. Najpomembneje, predstavijo strategijo, ki se lahko učinkotivto zoperstavi napadu bločnega prikrivanja v katerikoli rudarski skupini. Prvo priporočajo generično shemo, ki uporablja kriptografsko zavezujoče sheme za zoperstavitvi takemu napadu. Nato priporočajo alternativno implementacijo enake sheme z uporabo razpršilnih (angl. hash) funkcij. Taka shema ščiti skupino rudarjev pred zlonamernimi rudarji, tako navadnimi kot tudi administratorskimi redarji. Tako ta shema kot tudi druge njene različice ponujajo obrambo pred BWH napadi s tem, da onemogočijo možnost, da rudarji razlikujejo med celovitimi in delnimi dokazi dela. Prav tako pa te sheme omogočajo zaščito, da administratorji ni omogočeno goljufanje znotraj skupine katero nadzorujejo. Shemo se lahko implementira tako, da se napravi korenito spremembo na obstoječem Bitcoin protokolu. Na koncu se tudi posvetijo analizi varnosti opisane sheme.

Ključne besede: Bitcoin rudarjenje, napad z bločnim prikrivanjem, sebičen rudar, rudarske skupine, zavezujoče sheme.

1 Uvod

Bitcoin je popularna kripto valuta, ki jo je prvo priporočil Satoshi Nakamoto [1] leta 2008. Transakcije so javno preverljive v glavnem računu imenovanem "bločna veriga"(angl. blockchain). Bločna veriga je sestavljena iz veliko blokov, ki potrdi različne transakcije. Uporabniki, ki ustvarjajo in preverjajo te bloke se imenujejo rudarji. Rudarji nato kot motivacijo pridobijo novo ustvarjene Bitcoin-e. Da bi se reguliralo pretok Bitcoinov se bloki ustvarijo približno vsakih 10 minut. Rudarji morajo rešiti uganko (kot dokaz dela - angl. proof of work (PoW)), če hočejo pridobiti spodbudne Bitcoin-e. Čeprav obstajajo alternativne valute kot Permacoin [2] in Retriecoin [3], ki uporabljajo shrambe namesto računanja za ustvarjanje valute, je dokazovanje dela, ki ga uporablja Bitcoin zaenkrat še vedno najboljši načrt. V [4] so Kroll in drugi pokazali, da Bitcoin rudarjenje ni tako "končno", vodeno z vlogami in motivacijsko kompatibilen sistem kot pravijo nekateri njegovi zagovorniki. Napadi z bločnim prikrivanjem [5], [6]

2 Luka - page 5 and forth

α	β	γ	p'	$\triangle G_h^O$
0.200000	0.500000	0.700000	0.340000	0.248016
0.100000	0.900000	0.700000	0.400000	0.417396
0.200000	0.400000	0.700000	0.340000	0.214171
0.160000	0.600000	0.700000	0.330000	0.254052
0.200000	0.800000	0.700000	0.400000	0.394558
0.200000	0.900000	0.700000	0.400000	0.408747
0.200000	0.960000	0.700000	0.400000	0.414236
0.200000	0.990000	0.700000	0.400000	0.416150
0.200000	0.700000	0.700000	0.400000	0.415573

TABELA II: Tabelarični prikaz vrednosti $\triangle G_h^O$ za različne vrednosti ustreznih parametrov. α prikazuje računsko moč napadalca. β prikazuje del računske moči, ki jo napadalec uporabi pri napadu na bazen rudarjev P. γ prikazuje del spodbude, ki jo bazen P' pridobi zaradi napada napdalaca, ter jo z njim deli. p' predstavlja računsko moč P'.

Ker je 1 - $\alpha\beta$ dobiček P naraste $\frac{p'}{1-\alpha\beta}$. Torej je narastek dobička bazena rudarjev P' $\frac{p'}{1-\alpha\beta}$ - p' = $\frac{\alpha\beta p'}{1-\alpha\beta}$

Literatura

[1] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008. 2

[2] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, *Permacoin: Repurposing bitcoin work for data preservation*, in 2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014. IEEE Computer Society, 2014, pp. 475–490. 2

[3] B. Sengupta, S. Bag, S. Ruj, and K. Sakurai, *Retricoin: Bitcoin based on compact proofs of retrievability*, in Proceedings of the 17th International Conference on Distributed Computing and Net- working, ser. ICDCN '16, 2016, pp. 14:1–14:10. 2

[4] J. A. Kroll, I. C. Davey, and E. W. Felten, *The economics of bitcoin mining, or bitcoin in the presence of adversaries,*Proceedings of WEIS, vol. 2013, 2013. 2

[5] M. Rosenfeld, *Analysis of bitcoin pooled mining reward systems*, CoRR, vol. abs/1112.4980, 2011. [Online]. Available: http://arxiv.org/abs/1112.4980 2

[6] A. Laszka, B. Johnson, and J. Grossklags, *Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, ch. When Bitcoin Mining Pools Run Dry, pp. 63–77. 2

[7] . Eyal, *The miner's dilemma*, in 2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015. IEEE Computer Society, 2015, pp. 89–103.

[8] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, *On power splitting games in distributed computation: The case of bit- coin pooled mining*, in IEEE 28th Computer Security Foundations Symposium, CSF 2015, Verona, Italy, 13-17 July, 2015, C. Fournet, M. W. Hicks, and L. Vigano', Eds. IEEE Computer Society, 2015, pp. 397–411.

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

[10] I. Damgárd, *Lectures on Data Security: Modern Cryptology in The- ory and Practice.* Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, ch. Commitment Schemes and Zero-Knowledge Protocols, pp. 63–86.

[11] D. B. Okke Schrijvers, Joseph Bonneau and T. Roughgarde, *In- centive compatibility of bitcoin mining pool reward functions*, in Financial Cryptography and Data Security: FC 2016 International Workshops.

[12] S. Bag and K. Sakurai, *Yet another note on block withholding attack on bitcoin mining pools*, in Information Security - 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016, Proceedings, ser. Lecture Notes in Computer Science, M. Bishop and A. C. A. Nascimento, Eds., vol. 9866. 2016, pp. 167–180.