

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 kvantitativno 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 učinkovito 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 rudarji. Tako ta shema kot tudi druge njene različice ponujajo obrambo pred BWA 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 katere nadzorujejo. Shemo se lahko implementira tako, da se napravi korenito spremembo na obstoječem Bitcoin protokolu. Na koncu se tudi posvetijo analizi varnosti opisane sheme.

1 Uvod

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 [referenca] 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 [referenca] in Retriecoin [referenca], ki uporabljajo shrambe namesto računanja za ustvarjanje valute, je dokazovanje dela, ki ga uporablja Bitcoin zaenkrat še vedno najboljši načrt. V [referenca] 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 [referenca],[referenca] Bitcoin is a popular cryptocurrency first proposed by Satoshi Nakamoto [1] in 2008. The transactions are put in a publicly verifiable ledger called a blockchain. A blockchain consists of many blocks, which in turn verify multiple transactions. Users who create and verify blocks are called miners. Miners receive newly created Bitcoins as incentive. To regulate the flow of Bitcoins, blocks are created once in approximately 10 minutes. The miners have to solve a puzzle (as a proof of work - PoW) in order to claim the incentive. Though there are alternative currencies like Permacoin [2] and Retriecoin [3] that use storage as opposed to computation for minting currency, the proof of work used by Bitcoin is well recognized to be the best proof of work scheme as of now. In [4], Kroll et al. showed that Bitcoin mining is not "the fixed, rule-driven, incentive-compatible system" as some of its patronizers claim. Block withholding attacks [5], [6],

Literatura

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

bibitempermacoin A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, *Permacoin: Repurposing bitcoin work for data preservation*, in 2014 IEEE

LITERATURA

- Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014. IEEE Computer Society, 2014, pp. 475–490.
- [2] 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 Networking, ser. ICDCN '16, 2016, pp. 14:1–14:10.
 - [3] 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.
 - [4] M. Rosenfeld, *Analysis of bitcoin pooled mining reward systems*, CoRR, vol. abs/1112.4980, 2011. [Online]. Available: <http://arxiv.org/abs/1112.4980>
 - [5] 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.
 - [6] . 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.
 - [7] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, *On power splitting games in distributed computation: The case of bitcoin 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.
 - [8] N. T. Courtois and L. Bahack, *On subversive miner strategies and block withholding attack in bitcoin digital currency*, arXiv preprint arXiv:1402.1718, 2014.
 - [9] I. Damgård, *Lectures on Data Security: Modern Cryptology in Theory and Practice*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, ch. Commitment Schemes and Zero-Knowledge Protocols, pp. 63–86.
 - [10] D. B. Okke Schrijvers, Joseph Bonneau and T. Roughgarde, *Incentive compatibility of bitcoin mining pool reward functions*, in Financial Cryptography and Data Security: FC 2016 International Workshops.

LITERATURA

- [11] 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.