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 prikrivanjem blokov [5], [6], [7], [8] so zelo poznani in o njih se pogovarjajo na Bicoin forumih. V takem napadu, goljufivi rudarji poskušajo povečati njihove spodbude s tem, da zmanjšajo zmagovito verjetnost drugih rudarjev. V Bitcoin omrežju se nekaj rudarjev združi tako, da nastane skupina rududarjev oz. bazen rudarjev, da združijo svoje računske moči s ciljem, da proizvedejo centralo z ogromno računske moči. V takih bazeni rudarjev, mora vsak rudar redno predložiti dokaz dela administratorju bazena rudarjev, da dokaže svoje delo proti rešitvi, ki je povezana z Bitcoin blokom. Reševanje dokaza dela je manj zahtevno kot reševanje dokaza dela, ki lahko bil povezan z Bitcoin blokom. Le tem pravimo delni dokazi dela. Delni dokazi dela so nadmnožica Bitcoinovih dokazov dela, zato je celoten dokaz dela, ki lahko pridobi spodbudo v vrednosti 25BTC lahko tudi delni dokaz dela za kateriholi bazen rudarjev. Tako služijo ti delni dokazi dela dvem namenom. Prvič, da se preverja ali rudar zares porablja svoje računske vire za reševanje dokazovanje dela na Bitcoin sistemu. Drugič, računanje delnih dokazov je veljavno delo za reševanje Bitcoinovega dokaza dela in računanje delnih dokazov le teh ni nepotrebna poraa računske moči bazena rudarjev. Vendar računanje vseh delnih dokazov povzroči veliko obremenitve za upravitelja bazena rudarjev. To se lahko omeji tako, da se izbere določeno stopnjo zahtevnosti za delne dokaze.

Vsak rudar iz bazena rudarjev poskuša poiskati dokaz dela na množici tran-

sakcij, ki vsebuje začetno transakcijo bloka, katera loči to množico transakcij od množic transakcij drugih rudarskih bazenov ali samostojnih rudarjev. Ta začetna transakcija bloka omogoči administratorju bazena, da zahteva dobitno nagrado v primeru, da njegov bazen rudarjev zmaga v igri rudarjenja. Tako v primeru, da rudar, ki pripada nekemu P bazenu rudarjev, dobi rešitev uganke, ima dve možnosti. Lahko odda rešitev administratorju bazena, ali pa prikrije dejstvo, da je našel rešitev. Rudar dobljene rešitve ne more poslati Bitcoin omrežju preko drugega bazena rudarjev. Tudi če protokol omogoča rudarju, da odda block s celotnim dokazom dela neposredno na Bitcoin omrežje, bo bazen rudarjev kateremu pripada še vedno dobil nagrado zahvaljujoč začetni transakciji, ki je vključena v bloku.

V napadih s prikrivanjem blokov bo goljufivi rudar administratorju bazena rudarjev posredoval le delne dokaze dela, ki pa niso celoviti dokazi dela in tako skril celovite dokaze, ki jih izračuna. Administrator bazena se tako ne zaveda, da rudar prikriva odkrit blok in tako misli, da rudar kot vsak drugi rudar uporablja svojo računsko moč za reševanje dokaza dela uganke. Tako bazen, nezavedujoč se o zlonamernem delovanju rudarja, deli svoje dobičke z goljufivim rudarjem. Tako lahko zlonamerni rudar pridobi spodbude na račun poštenih rudarjev znotraj bazena, brez da bi naredil karkoli koristnega za bazen rudarjev v katerem sodeluje.

Napad s prikrivanjem blokov je bil prvo predlagan v [5]. V [9] Curtois in Bahack pokažeta, da lahko goljufivi rudar deluje nepošteno, le za svojo lasno korist in tako postavi ugled Bitcoina v nevarnost s posredno uporabo računske moči ostalih poštenih rudarjev za svoj lasten dobiček in hkrati prikrajša ostale rudarje za spodbudo, ki si jo zaslužijo. V [8] Luu in ostali podajo kvantitivno analizo koliko spodbude lahko rudar predvidoma poveča dobiček z izvajanjem napada s prikrivanjem blokov nad nekim bazenom rudarjev. Pokazali so, da do dobička pride, ker goljufivi rudar zmanjša verjetnost zmage bazena rudarjev, ki ga napada. S tem napadalec poveča svoje možnosti za zmago v Bitcoinovi igri rudarjev. Na dan 13. junij 2014 je bilo poročanje o razsežnem NPB (napad s prikrivanjem blokov) nad rudarskim bazenom Eligius [9], ki je povzročil izgube v višini 300BTC (Bitcoin valuta) na račun poštenih rudarjev.

V [6] Laszka in ostali priskrbijo na podlagi igre teoretično analizo napada s prikrivanjem blokov v katerih se pokažejo zanimivi rezultati o dolgolročni vzdržljivosti Nash ravnotežja med napadnjem bazenov v Bitcoin omrežju. Eyal in ostali [7] predlagajo rudarsko igro kjer se bazen rudarjev poskuša vtihotapiti v druge bazne rudarjev tako, da pošlje svoje posamezne rudarje v druge bazene rudarjev kjer potem sprožijo NPB na ciljne bazene rudarjev. Pokazali so, v primeru, da se dva ali več bazenov napada med seboj, bodo pošteni rudarji

zaslužili manj kot pričakujejo. V izvornem članku se o takem primeru tudi razpravlja. Vendar se delo avtorjev članka v [13] razlikuje od dela Eyal in drugih [7] na naslednje načine: (a) Avtorji članka se osredotočijo na znesek dobička, ki ga proizvede napadalec, ki sproži NPB nad nekim ciljnim bazenom rudarjev, katerega nagradi nek drugi bazen rudarjev, ker je napadalec napadel določen bazen rudarjev. Eyal in ostali izračunajo izraze prihodkov, ki jih proizvedejo bazeni rudarjev, ko je scenarij napada omrežja v sanju ravnotežja. (b) V modelu avtorjev [13] lahko napadalec razdeli svojo računsko moč in tako napada oba bazena rudarjev. Tako lahko prejme nagrade od obeh bazenov, katera nagradita napadalca, ker mislita, da je napadalec napadel le drugi bazen. Toda Eval in drugi razpravljajo scenarij napada kjer so napadalci člani bazena rudarjev in delijo prihodke pridobljene iz napadenega bazena z rudarji v goljufivem bazenu.

1.1 Motivacija in ostalo delo

TEst

Literatura

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

[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.

[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. 2, 3

[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. 2, 3

[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. 2, 3, 4

[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. 2, 3

[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. 3

[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.

[13] Samiran Bag, Sushmita Ruj and Kouichi Sakurai, *Bitcoin Block Withholding Attack : Analysis and Mitigation*, IEEE Transactions on Information Forensics and Security