Probability of double spend attack for network with non-zero synchronization time

Lyudmila Kovalchuk[1,2], Mariia Rodinko[1,3], Roman Oliynykov[1,3], Dmytro Kaidalov[1], and Andrii Nastenko[1]

[1]Input Output HK
[2]National Technical University of Ukraine ”Igor Sikorsky Kyiv Polytechnic Institute”
[3]V.N. Karazin Kharkiv National University

Introduction. In this paper, we obtained for the first time mathematically substantiated formulas for probability of a double spend attack on blockchain that is based upon Proof-of-Work consensus protocol and longest chain rule, for a network with a non-zero time of block propagation in the model with continuous time. Also, for the first time, it was shown that probability of such attack depends on the value equal to the product of the block propagation time and of the block generation intensity. The larger is this value, the larger is the attack success probability. Formulas obtained allow not only calculating of the attack success probability at various network parameters, but also to determine the number of confirmation blocks allowing reduction of the attack probability below some given small threshold, e.g. 10^{-3}.

Related work. The idea of the double spend attack appeared at the same time when the idea of the blockchain itself – for the first time this attack was described in the paper by Nakamoto [4]. The same paper proposed a method to withstand such attack, namely, generation of a certain number of confirmation blocks. Probability of the attack success was also calculated, depending on the network parameters and the number of confirmation blocks. Unfortunately, these calculations were made with serious probabilistic mistakes, one of which was replacement of a random variable by its mathematical expectation. As a result of this and other mistakes, the attack success probability appeared to be significantly underestimated.

In the papers [6, 5] and in some others, the authors also pointed out that the attack probability in the Nakamoto paper was underestimated, but failed to propose any alternative options having comprehensive mathematical substantiation. The paper [2] became the first where probability attack formulas were strictly proved. However, this paper also had certain drawbacks related not to strictness of presentation but to the model itself in the framework of which the results were obtained. The authors considered a simplified model of the network operation at assumption that the block delivery time is zero. Note that even at this simplifying assumption proofs of the obtained results appeared to be quite cumbersome.

The paper [1] presents estimation of the security threshold for the Bitcoin protocol in the model with discrete time, taking into account network delays.

The paper [3] was the first on to state how exactly the block propagation time affects security of the consensus protocol against the double spend attack. In particular, one of results of this paper were formulas for calculation of the security threshold — the minimal ratio of an adversary allowing completion of such attack with probability 1. Note that the larger the block propagation time in the network, the larger the security threshold differs (downward) from 50%.

This paper is a logical continuation of the paper [3]. We obtained strictly substantiated formulas for attack probability calculation that allowed not only explicit obtaining of attack success probability, but also calculating the number of confirmation blocks would be sufficient to ensure security against such attack. Using obtained analytical expressions for attack probability, we obtained the relevant numerical results that also appeared to be quite interesting.

Main results. Further we need the following notations. Let p_H, p_M be the hashrates of honest and malicious miners (full nodes), respectively, $p_H + p_M = 1$. Also define D_H block delivery time for honest miners (here we make an assumption to the benefit of a malicious miner, and consider that such malicious miner is well-synchronized). Then define α_H, α_M as block generation intensities (average numbers of blocks per second, generated by honest and malicious miner, respectively) for honest and malicious miners, $\alpha = \alpha_H + \alpha_M$. In these designations block creation times have exponential distributions with parameters α_H, α_M respectively. Also define values

$$p'_M = 1 - e^{-\alpha_M D_H} \cdot p_H;\; p'_H = e^{-\alpha_M D_H} \cdot p_H.$$

Next, define an auxiliary value

$$P_z(k) = \frac{p_H^n}{(z-1)!} \cdot \frac{e^{-\alpha_M z D_H} \cdot (\alpha_M z D_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(z-i+1)! \cdot C_k^i}{(\alpha z D_H)^i}, \text{for } z \in \mathbb{N}.$$

Theorem 1: the success probability of double spend attack after confirmation blocks is

$$P(z) = \begin{cases} 1, & \text{if } p'_M \geq p'_H; \\ 1 - \sum_{k=0}^{z} P_z(k)\left(1 - \left(\frac{p'_M}{p'_H}\right)^{z-k}\right), & \text{else.} \end{cases}$$

Calculation results. Table 1 presents the results obtained using Theorem 1. We calculate the minimal number z of confirmation blocks sufficient to make probability of success less than 10^{-3}.

Table 1: The results for $\alpha = 0.00167$ sec^{-1} (as for BTC) and various values of the block delivery times (measured in seconds) and malicious hashrate, and results from Nakamoto article [4], for comparison

p_H	$D_H = 0$ (Nakamoto)	$D_H = 15$	$D_H = 30$	$D_H = 60$	$D_H = 120$	$D_H = 180$
	z					
0.1	6 (5)	6	6	6	7	7
0.15	9 (8)	9	9	9	10	11
0.2	13 (11)	13	14	14	16	17
0.25	20 (15)	20	21	22	26	30
0.3	32 (24)	33	35	39	48	61
0.35	58 (41)	62	67	78	111	176
0.4	133 (89)	150	170	224	515	$P_{success} = 1$

Conclusion. The results obtained show that probability of the double spend attack increases with growth of the block delivery time and intensity of block generation. The larger the block delivery time, the larger the number of confirmation blocks to prevent the attack. Moreover, if the block delivery time is sufficiently large, then the attack probability will be 1 irrespective of the number of confirmation blocks, even when attackers are in the minority, as e.g. in the right lower cell of Table 1.

References

[1] Peter Gaži, Aggelos Kiayias, and Alexander Russell. Tight consistency bounds for bitcoin. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 819–838, 2020.

[2] Cyril Grunspan and Ricardo Pérez-Marco. Double spend races. *International Journal of Theoretical and Applied Finance*, 21(08):1850053, 2018.

[3] Lyudmila Kovalchuk, Dmytro Kaidalov, Andrii Nastenko, Mariia Rodinko, Oleksiy Shevtsov, and Roman Oliynykov. Decreasing security threshold against double spend attack in networks with slow synchronization. *Computer Communications*, 154:75–81, 2020.

[4] Satoshi Nakamoto. A peer-to-peer electronic cash system. 2008.

[5] Carlos Pinzón and Camilo Rocha. Double-spend attack models with time advantange for bitcoin. *Electronic Notes in Theoretical Computer Science*, 329:79–103, 2016.

[6] Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.