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.