

**Title:** Probability of double spend attack for network with non-zero time delay

**Author(s):** Lyudmila Kovalchuk, Mariia Rodinko, Roman Oliynykov,  
Dmytro Kaidalov and Andrii Nastenko

The paper presents the formulas for probability of a double spend attack on blockchain with Proof-of-Work consensus protocol for a network with a non-zero synchronization time. The results show that probability of a double spend attack depends essentially on the block delivery time and intensity of block generation. More precisely, the probability of such attack increases when the product of these two values increases. The analytical results obtained in this paper allow not only to calculate the exact value of attack probability, but also to define the minimal number of confirmation blocks sufficient to guarantee the security against this attack with an arbitrary preset probability value.