Decreasing Security Threshold Against Double Spend Attack in Networks with Slow Synchronization

Lyudmila Kovalchuk[1,2]
Joint work with Dmytro Kaidalov[1], Andrii Nastenko[1], Mariia Rodinko[1,3], Olexiy Shevtsov[1,3], Roman Oliynykov[1,3]

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

April 29th, 2019

Previous Works

- [Nak08, Ros14, PR16, GP17], – estimations of probability of double spend attack in model with continuous time and zero network delivery delay (prompt synchronization between honest miners);
- [SZ15, SLZ16] – observations that this probability significantly depends on a network delivery delay;
- [GKL15, GKL17] – asymptotic estimates of splitting attack probability in model with discrete time and non-zero network delivery delay;
- [PSS17] – some asymptotic properties of blockchain with limited delivery time;
- [KKN$^+$18] – building of (non-asymptotic) upper bounds of splitting attack probability in models with discrete time and different network delivery delays for honest and malicious miners.

Main Questions

- How exactly the **security threshold** depends on network parameters, especially, on **intensity** of block generation, honest miners' **ratio** and **network delivery delay**?
- What is the probability of **double spend attack** for network with given parameters?

Our Results

- Exact value for security threshold for network with arbitrary parameters.

  We obtained strictly proved expressions for the minimal ratio of adversary sufficient for attack is guaranteed to be successful. As we show, for some network parameters this ratio may be essentially lower than 50%. Using this result, it is possible to find the probability of double spend attack for network with arbitrary parameters.

- Maximum allowable block generation rate for network with arbitrary parameters (for which network is still secure against double spend attack).

  We obtained expressions for the maximal intensity of block creation, at which the network remains resistant to double spend attack.

Assumptions for The Model Presented

- Time is a continuous parameter.
- Synchronization time between honest miners is upper bounded by given arbitrary value.
- Adversary can:
  - delay block delivering for honest miners within this upper bound;
  - corrupt any nodes he choose at each moment (such that common ratio of corrupted nodes is not more than some given value).
- Synchronization time of the adversary is also a given arbitrary value and can be set to zero.
- Block generation rate is set to arbitrary value (both for honest miners and the adversary).
- The fraction of adversarial hashpower is arbitrary.

Designations and Definitions (I)

- α is the common intensity of block generation in network, $\alpha = \alpha_H + \alpha_M$;
- D_H, D_M are block delivery delays for honest miners and adversary, respectively, $D_M \leq D_H$;
- $\Delta = D_H - D_M \geq 0$ is the difference between network delivery delays;
- $p_H = \frac{\alpha_H}{\alpha}$ and $p_M = \frac{\alpha_M}{\alpha}$ are the ratios of honest miners and the adversary, respectively;
- $\gamma = \gamma(\alpha, \Delta) = \alpha \cdot \Delta$ is the average number of blocks generated by all miners during the time Δ.

Designations and Definitions (II)

Definition 1

For a given network with parameters α, α_H, α_M, D_H and D_M its *security threshold* p_{st} is the minimal adversary's ratio that guarantees success of a double spend attack (i.e. if the adversary's ratio is not less than p_{st}, then the probability of a successful attack is equal to 1).

Auxiliary Results (I)

Lemma 2

For the given network with parameters α, α_H, α_M, D_H *and* D_M *the probability* p'_M *that the next block will be created by an adversary is equal to*

$$p'_M = 1 - e^{-\alpha_M \Delta} p_H;$$

the probability p'_H *that the next block will be created by honest miners is equal to*

$$p'_H = e^{-\alpha_M \Delta} p_H.$$

Auxiliary Results (II)

Lemma 3

Let, at some point in time t_0, the branch created by the adversary be n blocks shorter than the branch created by honest miners. Denote as E_n the event that at some point in time $t > t_0$ an adversary was able to create a longer chain, and let $q_n = P(E_n)$. Then

$$q_n = \begin{cases} 1, & \text{if } p'_M \geq p'_H; \\ \left(\frac{p'_M}{p'_H}\right)^n, & \text{otherwise.} \end{cases} \tag{1}$$

Main Result I. Security Threshold (I)

Theorem 4

For a given network with the parameter γ, the security threshold p_{st} is the solution of the equation

$$1 - p_{st} = \frac{e^{\gamma \cdot p_{st}}}{2}. \tag{2}$$

Main Result I. Security Threshold (II)

In the following table we give numerical results for the security threshold for various values of $\gamma = \gamma(\alpha, \Delta) = \alpha \cdot \Delta$.

Table: Security Threshold for Various Values of Parameter $\gamma = \gamma(\alpha, \Delta) = \alpha \cdot \Delta$

γ	1/30	0.1	0.5	1	2
p_{st}	0.491737	0.475643	0.391798	0.314923	0.221427

Interpretation

E.g., for Bitcoin, if $\Delta = 20$ sec and $\alpha = 1/600$, we obtain $\gamma = 1/30$ and the security threshold is $p_{st} = 0.491737$. It means that if the adversary's ratio is not less than 0.491737, his attack will be successful with probability 1.

Main Result II. Upper Bound for Intensity of Block Generation

Theorem 5

For a given network with parameters p_H, p_M, Δ_H and Δ_M, the network is completely (with probability 1) vulnerable to a double spend attack if and only if the intensity α of block generation satisfies the following inequality:

$$\alpha \geq \frac{\ln(2 \cdot p_H)}{(1 - p_H)\Delta}$$

(or $\alpha \geq \frac{\ln 2p_H}{p_M \Delta}$, which is the same).

Numerical Results

In the next table we adduce the numerical results for the minimal value of intensity of block generation, at which the probability of a double spend attack is equal to 1, for various adversary's ratio.

Table: Minimal intensity α of block generation (for various adversary's ratios and various Δ), at which the probability of a double spend attack is equal to 1

p_M	Δ				
	1 sec	**5 sec**	**10 sec**	**20 sec**	**60 sec**
0.1	5.878	1.176	0.588	0.294	0.098
0.2	2.350	0.470	0.235	0.118	0.039
0.3	1.122	0.224	0.112	0.056	0.019
0.4	0.456	0.091	0.046	0.023	0.008
0.45	0.212	0.042	0.021	0.011	0.004

Interpretation

E.g., for Bitcoin, if $\Delta = 20$ sec and $p_M = 0.3$, the intensity may be increased by 33 times to 0.056 blocks per second. However, in this case the probability of unintentional fork will also increase, whereby a lot of work will be wasted.

Formula for calculation of double spend attack probability after z confirmation blocks:

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

$$\text{where } P_n(k) = \frac{p_H^n}{(n-1)!} \cdot \frac{e^{-\alpha_M n D_H} \cdot (\alpha_M n D_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(n-i+1)! \cdot C_k^i}{(\alpha n D_H)^i},$$

where α_H, α_M are the intensities of block generation by honest and malicious participants;
$\alpha = \alpha_H + \alpha_M$;
D_H is the network delivery delay for honest participants;
$p_H = \frac{\alpha_H}{\alpha}, p_M = \frac{\alpha_M}{\alpha}$ are hashrates of honest and malicious participants;
$p'_M = 1 - e^{-\alpha_M D_H} \cdot \frac{\alpha_H}{\alpha_M + \alpha_H} = 1 - e^{-\alpha_M D_H} \cdot p_H$;
$p'_H = e^{-\alpha_M D_H} \cdot \frac{\alpha_H}{\alpha_M + \alpha_H} = e^{-\alpha_M D_H} \cdot p_H$.
Using these results, the probability of a double spend attack and the number of confirmation blocks can be calculated.

Conclusions (I)

The paper shows how the intensity of block generation affects the network security, and exact analytical expressions are adduced for both the network security threshold and the upper bound of block generation intensity. At the same time, it is essential that increase in the intensity of block generation results in making the network vulnerable to attacks, and, also the number of orphan blocks is increased, i.e. the amount of wasted work is also increased.

Conclusions (II)

Consequently, the problem of fast transaction processing, which is becoming ever more important, cannot be solved in the "classical" blockchain. Therefore, more complex data structures should be used, like a DAG (Directed Acyclic Graph) that significantly increase the block generation rate (and, accordingly, the speed of transaction processing) without compromising the security level.


Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos.
The bitcoin backbone protocol: Analysis and applications.
Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applicaitons of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II,, pages 281–310, 2015.


Juan Garay, Aggelos Kiayias, and Nikos Leonardos.
The bitcoin backbone protocol with chains of variable difficulty.
In *Annual International Cryptology Conference*, pages 291–323. Springer, 2017.


Cyril Grunspan and Ricardo Pérez-Marco.
Double spend races.
CoRR, abs/1702.02867, 2017.


Lyudmila Kovalchuk, Dmytro Kaidalov, Andrii Nastenko, Oleksiy Shevtsov, Mariia Rodinko, and Roman Oliynykov.
Number of confirmation blocks for bitcoin and ghost consensus protocols on networks with delayed message delivery.
In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pages 42–47. ACM, 2018.


Satoshi Nakomoto.
A peer-to-peer electronic cash system.
online, 2008.


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


Rafael Pass, Lior Seeman, and Abhi Shelat.
Analysis of the blockchain protocol in asynchronous networks.

In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer, 2017.


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


Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar.
Spectre: A fast and scalable cryptocurrency protocol.
IACR Cryptology ePrint Archive, 2016:1159, 2016.


Yonatan Sompolinsky and Aviv Zohar.
Secure high-rate transaction processing in bitcoin.
Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers, 2015.