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

Lyudmila Kovalchuk
Input Output HK,
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
lyudmila.kovalchuk@iohk.io

Dmytro Kaidalov
Input Output HK
Kharkiv, Ukraine
dmytro.kaidalov@iohk.io

Andrii Nastenko
Input Output HK
Kharkiv, Ukraine
andrii.nastenko@iohk.io

Mariia Rodinko
Input Output HK,
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
mariia.rodinko@iohk.io

Oleksiy Shevtsov
Input Output HK,
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
oleksiy.shevtsov@iohk.io

Roman Oliynykov
Input Output HK,
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
roman.oliynykov@iohk.io

***Abstract*—We study probability change of double spend attack on Proof-of-Work consensus protocol depending on network parameters in the model with continuous time. We analyze effect of block generation intensity on the network vulnerability to the attack, and provide analytical expressions for the network security threshold and for the upper bound of block generation intensity.**

***Index Terms*—Blockchain, Bitcoin, consensus protocol, double spend attack**

I. Introduction

We consider the general model of a blockchain network with arbitrary consensus with one common property: a miner who creates the next block is chosen randomly from the set of all miners during the block generation process. The example of such consensus protocol is the Proof-of-Work protocol. After creating the block, the miner should share it among other participants of the network. This sharing process may take some non-zero time which depends on the network parameters.

At the same time, a situation may occur when malicious miners (adversaries) are consolidated into a large enough mining pool, which consists of multiple devices placed one-by-one, and, as a result, these devices are highly synchronized. Their synchronization time,compared to honest miners time, is close to zero. Thus the adversaries ratio that guarantees their success in a double spend attack may be essentially less than the ratio of honest miners, i.e. it may be less than 50%.

In this paper, we introduce the concept of threshold, that is the minimal adversaries ratio which provides a successful attack with probability 1. We obtained a strictly proved analytical expression for this threshold that demonstrates its dependence not only on the adversary's ratio, but also on such network parameters as time delays and intensity of block generation. This expression allows to get the relevant numerical results and to find the adversariesratio that is critical for a given network. On the other hand, it also allows defining the maximal intensity of block generation permitted for the given network without its complete vulnerability to the attack.

II. Related Work

For the first time, a double spend attack was described in the well-known paper by Nakamoto [1], where he also obtained expressions for attack probability (which were not entirely accurate). Later, more consistent results on the attack probability were obtained in other papers [2]–[4], and the paper [4] gives completely proved expressions for probability of such attack. However,the main drawback of these papers is that the results were obtained under the assumption on the time delay (i.e. the time between block creation and its sharing among all miners)to be equal to zero, that is not so for a real network. At the same time, some papers (e.g., [5], [6]) contain an observation that the probability of successful attack significantly depends on the time delay and intensity of block generation. In [7], [8],a problem of constructing asymptotic estimates of splitting attack probability for the model with non-zero synchronization time (equal for honest miners and the adversary) is considered with time being a discrete parameter. In [9] statements on asymptotic properties of the blockchain with limited block delivery time were obtained. However, at the moment, there is no published method to obtain exact values for the double spend attack probability depending on network parameters, in particular, on the synchronization time.

In our paper [10]. we succeeded to provide a partial answer to this question, having considered two special cases: when the synchronization time interval of the adversary is the same as that of honest miners, and when it is two times smaller. Note that these results were obtained for the model with discrete time, and that significantly simplifies the process of obtaining the results.

III. Our Results

In this paper, we give a complete answer to the question formulated with the most common assumptions on the network parameter values. The model, in which our results were obtained, has the following characteristics:

- time is a continuous parameter;
- synchronization time between honest miners is upper bounded by a given arbitrary value; moreover, the adversary can delay the block delivery for honest miners within this upper bound;
- synchronization time of the adversary is also a given arbitrary value and can be set to zero;
- block generation rate is set to an arbitrary value (both for honest miners and for the adversary);
- the share of adversarial hashpower is arbitrary.

We give strictly proved expressions for the minimal share of adversaries in the presence of which their attack is guaranteed to be successful. At the same time, depending on the network parameters, this ratio may be essentially smaller than 50%.

Using the results obtained, we also give a solution of another problem of current interest related to increase in block generation intensity.

We find, under certain network parameters, the limit up to which the block generation intensity can be increased so that the network is not completely vulnerable to attacks.

For all analytically obtained results we will provide numerical examples and the relevant graphics.

IV. Security Threshold: Definition, Analytic Expressions and Numerical Results

Let us recall that, according to our assumptions, the consensus protocol provides unpredictable block generation (i.e. the creator of the next block is unknown to all miners until the block is created).

Let us denote as α the general intensity of block generation in network,

$$\alpha = \alpha_H + \alpha_M,$$

where α_H, α_M are intensities of block generation by honest miners and by the adversary, respectively.

Also let us denote as D_H and D_M the time delays for honest miners and for the adversary, respectively. We make an assumption in favor of the adversary, and assume that $D_M \leq D_H$ (with the reverse inequality, the results can be obtained similarly, but in that case honest miners will have an advantage, and the adversary will need to control more than 50% to attack) and denote as $\Delta = D_H - D_M \geq 0$ the difference between time delays.

The values $p_H = \frac{\alpha_H}{\alpha}$ and $p_M = \frac{\alpha_M}{\alpha}$ are the ratio of honest miners and the adversary, respectively. In the case of the PoW consensus protocol, these values are equal to corresponding hashrates; for other protocols, the values are the ratio of some other resources.

In a particular case, when $D_H = D_M = 0$, the probability of a double spend attack is equal to 1 if and only if $p_M \geq 1/2$ (i.e. the adversaries ratio is not less than 50%). Hence the term "50% attack" means the attack which is guaranteed to be successful. It implies that $p_M = 1/2$ is the security threshold in this case.

However, for the general case the security threshold is to be determined in a more complicated way, with account of the network parameters.

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 adversarys ratio that guarantees success of a double spend attack (i.e. if the adversarys ratio is not less than p_{st}, then the probability of a successful attack is equal to 1).

Further we will obtain the exact value of the security threshold for the preset network parameters. For this purpose, we need to describe the following values and relations between them:

- T_H is a random variable that is equal to time spent by honest miners to create one block;
- T'_H is a random variable that is equal to time spent by honest miners to create one block and propagate it across all honest nodes in the network;
- T_M is a random variable that is equal to time spent by malicious miners to create one block;
- T'_M is a random variable that is equal to time spent by malicious miners to create one block and propagate it across all malicious nodes in the network.

Note that we make an assumption in favor to adversaries and assume that they obtain all blocks, even generated by honest miners, within time interval D_M.

As shown in [4], random values T_H and T_M have exponential distributions:

$$\begin{aligned} F_{T_H}(t) = P(T_H < t) = 1 - e^{\alpha_H t}, \\ F_{T_M}(t) = P(T_M < t) = 1 - e^{\alpha_M t}, \end{aligned} \tag{1}$$

for the parameters $\alpha_H > 0$, $\alpha_M > 0$.

In our notations, the following equalities hold:

$$T'_H = D_H + T_H, \; T'_M = D_M + T_M. \tag{2}$$

Let us denote by p_H the probability that honest miners create the next block before malicious miners do that(provided that they started creating this block simultaneously), and $p_M = 1 - p_H$ is the probability of the opposite event. According to [4],

$$p_H = \frac{\alpha_H}{\alpha_H + \alpha_M},\ p_M = \frac{\alpha_M}{\alpha_H + \alpha_M}. \tag{3}$$

Also denote as p'_H the probability that honest miners create the next block and propagate it across all nodes in the network (at least, across all honest nodes) before malicious miners do that, and as p'_M- the probability of the opposite event, $p'_M = 1 - p'_H$.

Then

$$p'_H = P(T'_H < T'_M),\ p'_M = P(T'_M < T'_H), \tag{4}$$

and $p'_H + p'_M = 1$.

Let us denote as $T'_H(i)$ time which honest miners need to create and propagate the i^{th} block, i.e. time between events "$(i-1)^{th}$ block is created and received by all honest participants" and "i^{th} block is created and received by all honest participants". Similarly to (2), we also can write the equality

$$T'_H(i) = T_H(i) + D_H. \tag{5}$$

Then $T'_H(i)$, $i \geq 1$ are independent identically distributed random variables with distribution functions

$$F_{T'_H(i)}(t) = F_{T'_H}(t) = F_{T_H}(t - D_H) = 1 - e^{-\alpha_H(t-D_H)},$$
$$\text{for all } i \geq 1,\ t \geq D_H,$$

where the latter equality follows from (1).

Similarly, we define the random variables $T_M(i)$, $i \geq 1$, with distribution functions

$$F_{T_M(i)}(t) = 1 - e^{-\alpha_M t},\ \text{for all } i \geq 1.$$

Also, for $n \geq 1$ let us define random variables $S_H(n)$, where

$$S_H(n) = \sum_{i=1}^{n} T_H(i), \tag{6}$$

and random variables $S'_H(n)$, where

$$S'_H(n) = \sum_{i=1}^{n} T'_H(i). \tag{7}$$

Then $S_H(n)$ is the time needed for generation (on condition of zero synchronization time) of n independent blocks by honest miners, and $S'_H(n)$ is the time that is needed for honest miners to create and propagate consistently n blocks across the network.

From (5) we obtain:

$$S'_H(n) = S_H(n) + nD_H,$$

where $S_H(n)$ has the Erlang distribution (as a sum of identically distributed random variables with exponential distribution, [11], [12]):

$$F_{S_H(n)}(t) = P(S_H(n) \leq t) = 1 - e^{-\alpha_H t} \sum_{i=1}^{n} \frac{(\alpha_H t)^k}{k!}. \tag{8}$$

Similarly, let us define random variables $S_M(n)$ and $S'_M(n)$:

$$S_M(n) = \sum_{i=1}^{n} T_M(i),$$

$$S'_M(n) = \sum_{i=1}^{n} T'_M(i) = S_M(n) + nD_M. \tag{9}$$

A random variable $S_M(n)$ is also a sum of independent exponentially distributed random variables, so it also has the Erlang distribution [11], [12]:

$$F_{S_M(n)}(t) = P(S_M(n) \leq t) = 1 - e^{-\alpha_M t} \sum_{i=1}^{n} \frac{(\alpha_M t)^k}{k!}. \tag{10}$$

For a fixed $t \geq 0$, let us define a random variable $N'_M(t)$ as a number of blocks that were created and propagated across the network by an adversary during time t.

Now we can formulate and prove two auxiliary lemmas needed to obtain the main result.

Lemma 1. *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

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

Proof. According to (2) and (4), the distribution functions of random variables T'_H and T'_M are as follows:

$$F_{T'_H}(t) = P(T'_H < t) = P(T_H + D_H < t) =$$
$$= P(T_H < t - D_H) = \begin{cases} 1 - e^{-\alpha_H(t-D_H)}, & \text{if } t > D_H, \\ 0, & \text{otherwise;} \end{cases}$$

$$F_{T'_M}(t) = P(T'_M < t) = P(T_M + D_M < t) =$$
$$= P(T_M < t - D_M) = \begin{cases} 1 - e^{-\alpha_M(t-D_M)}, & \text{if } t > D_M, \\ 0, & \text{otherwise.} \end{cases}$$

Respectively, densities of these distributions are the following functions:

$$f_{T'_H}(t) = \alpha_H e^{-\alpha_H(t-D_H)};$$
$$f_{T'_M}(t) = \alpha_M e^{-\alpha_M(t-D_M)}. \tag{11}$$

The second equality in (4) can be rewritten as:

$$p'_M = P(T'_M < T'_H) = P(T_M + D_M < T_H + D_H) =$$

$$= P(T_M < T_H + D_H - D_M).$$

Let us define a random variable ζ, $\zeta = T_H + \Delta$.
Then

$$F_\zeta(x) = F_{T_H}(t - \Delta) = \begin{cases} 1 - e^{-\alpha_H(t-\Delta)}, & \text{if } t \geq \Delta; \\ 0, & \text{otherwise;} \end{cases}$$

$$f_\zeta(t) = \begin{cases} \alpha_H \cdot e^{-\alpha_H(t-\Delta)}, & \text{if } t \geq \Delta; \\ 0, & \text{otherwise.} \end{cases}$$

Hence $f_\zeta(t) = f_{T_H}(t - \Delta)$.

Taking into account these notations and using the compound probability formula, we obtain:

$$\begin{aligned} p'_M = P(T_M < T_H + \Delta) = \\ = P(T_M < T_H + \Delta / T_M < \Delta) P(T_M < \Delta) + \\ + P(T_M < T_H + \Delta / T_M > \Delta) P(T_M > \Delta). \end{aligned} \tag{12}$$

However,

$$\begin{aligned} P(T_M < T_H + \Delta / T_M < \Delta) = 1, P(T_M < \Delta) = \\ = 1 - e^{-\alpha_M \Delta,} \text{ and} \\ P(T_M < T_H + \Delta / T_M > \Delta) P(T_M > \Delta) = \\ = P(\Delta < T_M < T_H + \Delta). \end{aligned}$$

Let us compute the latter probability:

$$\begin{aligned} P(\Delta < T_M < T_H + \Delta) = \\ = \int_{x,y:\Delta<x<y} f_{T_M}(x) f_\zeta(y) dx dy = \\ = \int_\Delta^\infty \left(\int_\Delta^y f_{T_M}(x) dx \right) f_\zeta(y) dy = \\ = \int_\Delta^\infty (F_{T_M}(y) - F_{T_M}(\Delta)) f_{T_H}(y - \Delta) dy = \\ = \int_\Delta^\infty \left(1 - e^{-\alpha_M y} - \left(1 - e^{-\alpha_M \Delta} \right) \right) \alpha_H e^{-\alpha_H (y-\Delta)} dy = \\ = \int_\Delta^\infty \left(e^{-\alpha_M \Delta} - e^{-\alpha_M y} \right) \alpha_H e^{-\alpha_H (y - \Delta)} dy = \\ = \alpha_H e^{-\alpha_M \Delta} \int_\Delta^\infty \left(1 - e^{-\alpha_M (y - \Delta)} \right) e^{-\alpha_H (y - \Delta)} dy = \\ = \alpha_H e^{-\alpha_M \Delta} \int_0^\infty \left(1 - e^{-\alpha_M z} \right) e^{-\alpha_H z} dz, \end{aligned}$$

where $z = y - \Delta$.

After integration we obtain:

$$P(\Delta < T_M < T'_H) = e^{-\alpha_M \Delta} \cdot \frac{\alpha_M}{\alpha_H + \alpha_M},$$

and substituting the resulting expression into the formula (9), we obtain:

$$\begin{aligned} p'_M = 1 - e^{-\alpha_M \Delta} + e^{-\alpha_M \Delta} \cdot \frac{\alpha_M}{\alpha_H + \alpha_M} = \\ = 1 - e^{-\alpha_M \Delta} \cdot \left(1 - \frac{\alpha_M}{\alpha_H + \alpha_M}\right) = 1 - e^{-\alpha_M \Delta} \cdot \frac{\alpha_H}{\alpha_H + \alpha_M} = \\ = 1 - e^{-\alpha_M \Delta} \cdot p_H. \end{aligned}$$

So, $p'_H = 1 - p'_M = e^{-\alpha_M \Delta} \cdot p_H$. □

Lemma 2. *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*

$$q_n = \begin{cases} 1, & \textit{if } p'_M \geq p'_H; \\ \left(\frac{p'_M}{p'_H} \right)^n, & \textit{otherwise.} \end{cases} \tag{13}$$

Proof. According to the compound probability formula:

$$\begin{aligned} q_n = P(E_n) = P(E_n / T'_H > T'_M) P(T'_H > T'_M) + \\ + P(E_n / T'_H < T'_M) P(T'_H < T'_M) = \\ = P(E_{n-1}) p'_M + P(E_{n-1}) p'_H, \end{aligned}$$

where the latter equality was obtained using Theorem 1.

So,

$$q_n = q_{n-1} p'_M + q_{n-1} p'_H. \tag{14}$$

To solve the equation (14), we write the corresponding difference equation:

$$\lambda^2 p'_H - \lambda + p'_M = 0,$$

whose roots are $\lambda_1 = 1$ and $\lambda_2 = \frac{p'_M}{p'_H}$. Then the general solution of (14) is

$$q_n = a\lambda_1^n + b\lambda_2^n = a + b\left(\frac{p'_M}{p'_H} \right)^n.$$

If $p'_M > p'_H$, then $\frac{p'_M}{p'_H} > 1$. But, according to the definition of q_n, the condition $0 \leq q_n \leq 1$ holds. So, in this case $b = 0$, $a = 1$, and the only solution of (14) is $q_n = 1$.

If $p'_M = p'_H = 1/2$, then we obtain the equation $\Lambda^2 - 2\lambda + +1 = 0$, whence $\lambda_1 = \lambda_2 = 1$ and $q_n = 1$ for all $n \geq 1$, with account of the initial condition $q_0 = 1$.

Finally, if $p'_M < p'_H$, then from the boundary conditions $q_0 = 1$, $q_\infty = 0$ we obtain $a = 0$, $b = 1$, and $q_n = \left(\frac{p'_M}{p'_H} \right)^n$. □

Now we can prove the main result of this section.

Let us denote as $\gamma = \gamma(\alpha, \Delta)$ the average number of blocks generated by all miners during the time Δ:

$$\gamma = \gamma(\alpha, \Delta) = \alpha \cdot \Delta.$$

Theorem 1. *For a given network with the parameter γ, the security threshold p_{st} is the solution of the equation*

$$1 - p_{st} = \frac{e^{\gamma \cdot p_{st}}}{2}. \tag{15}$$

Proof. Let B be a block on which the double spend attack is performed; z is the number of confirmation blocks after the block B. Let us define the event $A_z(k)$ in the following way:

$$A_z(k) = \{N_M(S'_H(z) = k)\} = \{X'_M(z) = k\},\ k \geq 0,$$

where $X'_M(n) = N_M(S'_H(n))$.

In other words, the event $A_z(k)$ is as follows: "the adversary created and propagated exactly k blocks, while honest miners created and propagated z confirmation blocks".

Also, let us define the event A_z as "the adversary was able to build a longer chain after the block B received z confirmation blocks". Then

$$A_z = \left\{ \bigcup_{k \geq z} A_z(k) \right\} \cup \left\{ \bigcup_{k=0}^{z-1} \Big(A_z(k) \cap E_{n-k} \Big) \right\}, \tag{16}$$

where E_{z-k} is as defined in Lemma 1.

Note that the events $\{\bigcup_{k \geq z} A_z(k)\}$ and $\{\bigcup_{k=0}^{z-1} (A_z(k) \cap E_{n-k})\}$ do not intersect, and the events $A_z(k)$ and E_{n-k} are independent. Besides, according to Lemma 1:

$$P(E_{z-k}) = \begin{cases} 1, & \text{if } p'_M \geq p'_H; \\ \frac{p'_M}{p'_H}, & \text{otherwise.} \end{cases} \tag{17}$$

So, taking into account (16), we obtain:

$$P(A_z) = \sum_{k=z}^{\infty} P\big(A_z(k)\big) + \sum_{k=0}^{z-1} P\big(A_z(k)\big) P\big(E_{z-k}\big).$$

From the latter equality, taking into account (17), and that $\sum_{k=0}^{\infty} P\big(A_z(k)\big) = 1$, we obtain:

$$P(A_z) = \begin{cases} \sum_{k=z}^{\infty} P\big(A_z(k)\big) + \\ + \sum_{k=0}^{z-1} P\big(A_z(k)\big) \left(\frac{p'_M}{p'_H} \right)^{z-k}, & \text{if } p'_M < p'_H; \\ 1, & \text{otherwise.} \end{cases} \tag{18}$$

That is, the attack probability is equal to 1 if and only if $p'_M \geq p'_H$. This condition is equivalent to the condition $p'_M \geq 1/2$. Using Lemma 1, we can rewrite this inequality as

$$1 - e^{-\alpha_M \Delta} p_H \geq \frac{1}{2},$$

that with an elementary transformations can be reduced to the inequality

$$2(1 - p_M) \leq e^{\alpha p_M \Delta}. \tag{19}$$

That is, the value p_0 is the minimal value of p_M, for which the inequality (19) holds, i.e. p_0 is the solution of the equation $2(1 - p_M) \leq e^{\alpha p_M \Delta}$, that we were to prove. □

In Table 1 we give numerical results for the security threshold for various values of $\gamma = \gamma(\alpha, \Delta) = \alpha \cdot \Delta$.

Fig. 1 shows dependence of security threshold on the parameter γ.

TABLE I
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

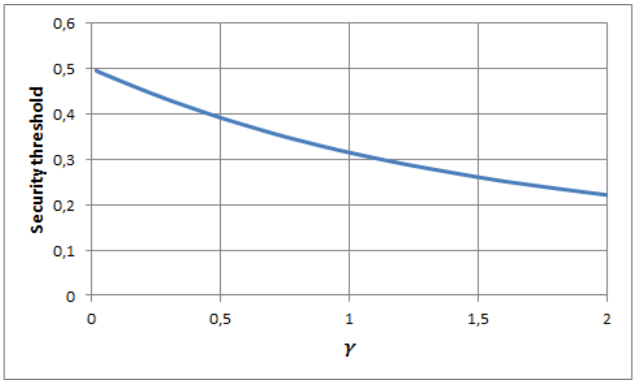

Fig. 1. Dependence of Security Threshold on the Parameter $\gamma = \Delta\alpha_H$ (the product of time delay difference and intensity of block generation)

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 adversarys ratio is not less than 0.491737, his attack will be successful with probability 1.

V. SOLUTION OF THE INVERSE PROBLEM: FINDING UPPER BOUNDS FOR INTENSITY OF BLOCK GENERATION

Using Theorem 1, we also may solve another important problem: to determine the maximal intensity of block creation at which the network remains resistant to a double spend attack. Theorem 2 gives the solution of this problem.

Theorem 2. *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 equality:*

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

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

In Table 2 we adduce the numerical results for the maximal value of intensity of block generation, at which the network remains resistant to a double spend attack, for various adversarys ratios.

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.

VI. CONCLUSIONS

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

TABLE II
MAXIMAL INTENSITY α OF BLOCK GENERATION FOR VARIOUS ADVERSARYS RATIOS AND VARIOUS Δ

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

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.

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, [5], [6], [13], [14]) or Parallel Chains [15] that significantly increase the block generation rate (and, accordingly, the speed of transaction processing) without compromising the security level.

REFERENCES

[1] S. Nakomoto, “A peer-to-peer electronic cash system,” *online*, 2008.

[2] M. Rosenfeld, “Analysis of hashrate-based double spending,” *arXiv preprint arXiv:1402.2009*, 2014.

[3] C. Pinzon and C. Rocha, “Double-spend attack models with time advantange for bitcoin,” *Electronic Notes in Theoretical Computer Science*, vol. 329, pp. 79–103, 2016.

[4] C. Grunspan and R. Pérez-Marco, “Double spend races,” *CoRR*, vol. abs/1702.02867, 2017.

[5] Y. Sompolinsky and A. 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.

[6] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, “Spectre: A fast and scalable cryptocurrency protocol.,” *IACR Cryptology ePrint Archive*, vol. 2016, p. 1159, 2016.

[7] J. A. Garay, A. Kiayias, and N. 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,*, pp. 281–310, 2015.

[8] J. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol with chains of variable difficulty,” in *Annual International Cryptology Conference*, pp. 291–323, Springer, 2017.

[9] R. Pass, L. Seeman, and A. Shelat, “Analysis of the blockchain protocol in asynchronous networks,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 643–673, Springer, 2017.

[10] L. Kovalchuk, D. Kaidalov, A. Nastenko, O. Shevtsov, M. Rodinko, and R. 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*, pp. 42–47, ACM, 2018.

[11] W. Feller, *An Introduction to Probability Theory and its Applications*. New York: Wiley, 1970.

[12] S. Karlin, H. E. Taylor, and H. M. Taylor, *A First Course in Stochastic Processes*, vol. 1. Gulf Professional Publishing, 1975.

[13] Y. Sompolinsky and A. Zohar, “Phantom: A scalable blockdag protocol,” 2018.

[14] S. Popov, “The tangle (2017),” *URL https://iota. org/IOTA_Whitepaper. pdf.*

[15] M. Fitzi, P. Gaži, A. Kiayias, and A. Russell, “Parallel chains: Improving throughput and latency of blockchain protocols via parallel composition.” Cryptology ePrint Archive, Report 2018/1119, 2018.