УДК 517.4: 004.056

Comparison of efficiency of Double Spend Attack for blockchains with checkpoints and without them

Lyudmila Kovalchuk[1], Nataliia Kuchynska[2], Hanna Nelasa[3]

[1] Doctor of Technical Sciences, Professor, Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine, 15 General Naumova Str., 03164, Kyiv, Ukraine e-mail: lusi.kovalchuk@gmail.com
[2] Candidate of Technical Sciences, Associate Professor, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37, Prosp. Peremohy, 03056, Kyiv, e-mail: n.kuchinska@gmail.com
[2] Candidate of Technical Sciences, Associate Professor, Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine, 15 General Naumova Str., 03164, Kyiv, Ukraine e-mail: annanelasa@gmail.com

Though Proof-of-Stake (PoS) protocol is widely-used in blockchains, but the first strictly proved results about its security against Double Spend Attack (DSA) were recently obtained. To reduce the probability of this attack, some blockchains use some additional instrument, which is called checkpoints. In this paper, we present explicit formulas for the estimates of probability of success of Double Spend Attack in the case of the Proof of Stake protocol consensus with checkpoints and compare obtained results with probability of classic Double Spend Attack. The formulas obtained allow to get corresponding numerical results, which we compared with the analogical numerical results obtained earlier for "classical" PoS protocol in blockchain without checkpoints. As it was expected, this comparison shows that blockchain with checkpoints, under the same conditions, is more secure against such attack.

Key words: blockchain; double spend attack, proof of stake, checkpoint

Introduction. The main cryptographic principles of modern blockchain technology were proposed by Satoshi Nakomoto in 2008, the idea was practically implemented only in 2009 in the first cryptocurrency Bitcoin. Consensus protocols are not completely reliable because the partial centralization can occur in the system when the consensus models do not take into account behavior of the network users. To increase the blockchain security a checkpoint mechanism was proposed [1] [2]. It is called to limit the time of the attack. Once the chain history is synced, it cannot be changed.

1. Double Spend Attack with time limitations

In this paper a partial case of Double Spend Attack is considered. In further we assume the malicious miners have limited time to implement the attack and the one block is built during one timeslot. This model depends on the distribution of timeslots in blockchain between network participants. By limitations on the time of the attack, we suppose the presence of checkpoints. The number of timeslots between control points is assumed to be known. The selection of slot leaders for the corresponding slots between checkpoints is random in our assumptions.

As in the case of the classic DSA for the proof of stake consensus protocol, the attack should be divided into two stages. The first stage is that the attacker will build an alternative chain before honest miners build z of confirmation blocks. The second stage of the attack occurs when z blocks of confirmation are built and the attacker was

unable to carry out the attack in its first stage, he lags behind by a certain number of z − k blocks (k is the number of blocks built by the attacker), and therefore the attackers pass to the phase when there is an attempt to catch up with the main chain. But it is necessary to catch up before the second checkpoint, since after it his fork will not be considered valid.

Compared to the classic case of DSA, in the control point attack, everything follows the same assumptions as described in [3], but the opponent can catch up in a limited number of slots. In order to prove new statements and formulas, it is necessary to introduce next notations.

Let through $B_0^{x_0}, B_0^{x_1}, B_0^{x_2}, \ldots, B_{i-1}^{x_{i-1}}, B_i^{x_i}, \ldots, B_{2n}^{x_{2n}}$, $i \in N$, $x_i \in \{H, M\}$ we will denote the slots on each of which the selected slot leader can build only one block. That is, the timeslots will belong to a certain selected slot leader, which will be indicated in the index above the specified designations, where H is the slot of honest miners and M is the slot of malicious miners. If the indexing of slot numbers is marked in round brackets, then this designation will mean the ordering of the slot data belonging to a certain slot leader.

By $B_{(0)}^H, B_{(1)}^H, \ldots, B_{(i)}^H, \ldots$ we denote the selected timeslots on which the blocks are built by honest miners. Let's introduce the transaction X, included in the block $B_{(i)}^H$, $i \in N$, which consists in the fact that the attacker transferred funds to the supplier for goods or a certain service. To carry out a transaction for payment of a service or product, the supplier must wait z blocks of confirmation after the block $B_{(i)}^H$. The creation of z blocks of confirmation is done in order to ensure greater security of blockchain systems, which makes it impossible to replace the main chain with the block $B_{(i)}^H$ for an alternative one with the transaction Y.

Let there be an attack on the blockchain system, and the formation of a fork, that is, a branching, from the block $B_{i-1}^{x_{i-1}}$, which precedes the block $B_{(i)}^H$ with transaction X. There are two chains when attacking. The main chain is built only by honest miners:

$$B_0^{x_0}, B_0^{x_1}, B_0^{x_2}, \ldots, B_{i-1}^{x_{i-1}}, B_{(i)}^H, B_{(i+1)}^H, B_{(i+2)}^H, \ldots, B_{(i+z)}^H,$$

where blocks starting from $B_{(i)}^H$ are built only by honest miners, and the alternative chain, where blocks starting from $B_{(i)}^M$ are built only by a malicious miner.

$$B_0^{x_0}, B_0^{x_1}, B_0^{x_2}, \ldots, B_{i-1}^{x_{i-1}}, B_{(i)}^M, B_{(i+1)}^M, \ldots, B_{(r)}^M,$$

An alternative chain is built in secret as long as it is smaller in number of blocks than the main chain $r < z$, that is, the construction of the malicious chain begins after z blocks $B_{(i+1)}^H, B_{(i+2)}^H, \ldots, B_{(i+z)}^H$ confirmation. The chain must start before block $B_{(i)}^H$ otherwise the block with transaction Y will contain an invalid transaction that uses already spent coins. The attacker does not have the right to build his blocks in the chain of honest miners during the attack. In order to carry out a successful attack, the

alternative chain must be longer or at least equal to the main chain when posting the malicious chain to the blockchain network.

Since the history of the blockchain will be synchronized every $2n$ timeslots, the attack should be carried out in the interval between the given number of timeslots. As an example, let a checkpoint occur in timeslot $B_{(\mathrm{i}+2\mathrm{n})}^{x_{i+2n}}$, it will synchronize the state of the network at the checkpoint with block $B_{(\mathrm{i}+\mathrm{n})}^{x_{i+n}}$. The attack should be carried out in the timeslot with the block $B_{(\mathrm{i})}^{x_i}$, otherwise if it is the timeslot with the block $B_{(\mathrm{i}+\mathrm{n}-1)}^{x_{i+n-1}}$, then the newly formed fork will be rejected by the network at the control point that occurs in the timeslot with the $B_{(\mathrm{i}+\mathrm{n})}^{x_{i+n}}$ block, and the attack will be doomed to failure. So, we will consider DSA assuming that it was carried out after the first control point.

Assuming the existence of checkpoints for DSA, honest and malicious miners should now probably hit timeslots whose number is only $2n$, accordingly, the attack can be successfully carried out if $r+z \le 2n$ while the number of blocks of the attacker has be $r \ge z$ at the time of publishing your chain. If more blocks are built by honest or malicious miners in more timeslots, then the attack must be carried out again after the checkpoint. Because the probability of an attack after the checkpoint is zero and the synchronized history of the chain is already firmly stored in the blockchain system, it cannot be changed in any way. Now that you have an idea of the mechanism of checkpoints, you can proceed to the mathematical formulation of the model.

Suppose that among x participants exactly $t\left(t < x/2\right)$ are criminals and $x-t$ are honest. Then, $p=(x-t)/x$ is the probability that the next timeslot belongs to an honest miner, and $x=t/x$ is the probability of an alternative event.

By $\xi_i, i \ge 1$ – denote random variables that can take only two values:

$$\xi = \begin{cases} -1 \text{ with probabilit y q timeslot of an honest miner,} \\ 1 \text{ with probabilit y p the timeslot of the malicious.} \end{cases} \tag{1}$$

Let's define random variables:

$$S_0 = 0,\ S_n = \sum_{i=1}^{n} \xi_i\ , \tag{2}$$

$$S_0^+ = 0,\ S_n^+ = \sum_{i=1}^{n} (\xi_i \vee 0)\ , \tag{3}$$

$$S_0^- = 0,\ S_n^- = \sum_{i=1}^{n} (-\xi_i \vee 0)\ . \tag{4}$$

Let's write down the sense of this random variables:

- $S_n^+,\ n = 0,1...$ – is equal to the number of timeslots that an honest slot leader has in the interval between the slot numbered 0 and the slot numbered n;
- $S_n^-,\ n = 0,1...$ – similar value of the number of slots of the opponent;
- $S_n,\ n = 0,1...$ is the difference $S_n^+ - S_n^-$ between honest and dishonest slot leaders.

For some $k \in N$, we define another random variable $\tau_k = \min\{l \geq 1 : S_l^+ = k\}$. Here, τ_k is the number of timeslots such that on the interval $[0, \tau_k]$ there are exactly k slots owned by honest slot leaders. Now the problem of calculating the probability of attack success can be formulated as the problem of calculating the probability of the next event:

$$A(k) = \{\exists m \geq \tau_k : S_m^- \geq S_m^+\},$$

where for $k = z$ and S_m^-, S_m^+ are defined according to 1-4.

A further proof of the DSA probability formula with checkpoints will no longer require a result concerning random walks, namely the player's ruin lemma. It is necessary to consider the finite case of the game, which will be presented in combinatorial reasoning.

Lemma 1. In the notation (1)-(4) we define random variables:
$S_n^{(k)} = S_n + k, S_0^{(k)}, S_0^{(k)} = k$.

We also define the event $C_k = \{\exists l \in N : S_l^{(k)} = 0\}$ and denote its probability by $q_k = P(C_k)$. If the attacker has a share q in the blockchain network, which is less than the share of the honest p, but not very significantly, and at the same time the alternative chain lags behind the main one by $z - k$ blocks behind, then the probability of the attacker catching up with the main chain if there is in the blockchain system, checkpoints after every n time slots are calculated according to the formula:

$$q_k = \sum_{i=0}^{n-z} \left(C_{z-k+2i}^i p^i q^{z-k+i} - \sum_{j=0}^{i-1} p_i C_{2i-2j}^{i-j} (pq)^{i-j} \right).$$

Theorem 1. The probability of the DSA in the PoS consensus protocol in the presence of checkpoints is calculated by the recursive formula:

$$P(A(z)) = \sum_{k=0}^{z-1} C_{z+k-1}^k p^z q^k \sum_{i=0}^{n-z} p_i + \sum_{k=z}^{2n-z} C_{z+k-1}^k p^z q^k,$$

where $p_k = C_{z-k+2i}^i p^i q^{z-k+i} - \sum_{j=0}^{i-1} p_i C_{2i-2j}^{i-j} (pq)^{i-j}$.

2. Practical confirmation of the obtained results

If the attacker is limited checkpoints, he cannot build an arbitrary number of blocks. For protect against the DSA in such conditions it is necessary to find the number of confirmation blocks for which the probability of the attacker's success will be negligibly small. After the checkpoint, the probability of implementation of attack will be zero.

Our computations results are the different values of probabilities for an attack on the blockchain with checkpoints were obtained in case when the number of timeslots between checkpoints is limited. There are also blockchains with checkpoints, where the distance between checkpoints is calculated in a limited number of blocks, duration of time, number of days. This paper does not consider checkpoints with a fixed number

of blocks between checkpoints or waiting for a certain time interval. These partial cases of modification of the checkpoint mechanism are separate topics for future research.

The obtained probabilities of an attack on a blockchain system with checkpoints describe the case of DSA when there are 50, 150, 300 time slots between the checkpoints, respectively. Comparison to the classic DSA and an attack on a blockchain system with checkpoints shows that checkpoints allow to reduce the probability of an attack, and this comparison also allows to check the adequacy of the obtained results.

Conclusions In this paper, for the first time were obtained explicit formulas for calculating the probability of DSA for PoS consensus protocol in case of blockchain with checkpoints. Also we got a large number of numerical results, which confirmed the correctness of analytical ones.

The numerical results indicate that the probability of DSA for blockchain with checkpoints is smaller than for blockchain without them; the smaller distance between checkpoints, the smaller probability of attack; the larger ratio of malicious participants, the larger difference between probabilities of attack for blockchain with checkpoints and for blockchain without them.

So, it can be concluded that for various financial transactions with cryptocurrencies, it is justified to advise the seller of a product or service to wait for the number of confirmation blocks that can be built as much as possible between two checkpoints, but in an amount that does not exceed the number of blocks between two checkpoints. In this case, an attack on such a network is expected to be impossible in a practical sense.

References

[1] Sunny King S N 2012 Computer Science, Mathematics URL http://www.peercoin.net/
[2] Gencer A E, Van Renesse R and Sirer E 2017 Short paper: Service-oriented sharding for blockchains Lecture Notes in Computer Science pp 393–401 ISBN 978-3-319-70971-0
[3] Karpinski M, Kovalchuk L, Kochan R, Oliynykov R, Rodinko M and Wieclaw L 2021 Sensors 21 ISSN 1424-8220 URL https://www.mdpi.com/1424-8220/21/19/6408

Порівняння ефективності Double Spend Attack для блокчейнів з контрольними точками і без них

Людмила Ковальчук, Наталія Кучинська, Ганна Неласа

Хоча протокол Proof-of-Stake (PoS) широко використовується в блокчейнах, перші чітко підтверджені результати щодо його стійкості до Атаки Подвійної Витрати (АПВ) були отримані лише нещодавно. Щоб зменшити ймовірність цієї атаки, деякі блокчейни використовують додатковий інструмент, який називається контрольними точками. У цій роботі ми представляємо явні формули для оцінки ймовірності успіху АПВ у випадку протоколу консенсусу Proof of Stake з контрольними точки та порівнюємо отримані результати з відповідними для класичної АПВ. Запропоновані формули дозволяють отримати відповідні числові результати, які ми порівняли з аналогічними числовими результатами, отриманими раніше для «класичного» протоколу PoS в блокчейні без контрольних точок. Як і очікувалося, це порівняння показує, що блокчейн з контрольними точками за однакових умов є більш стійким до такої атаки.

Received 14.03.23