# SECURITY ANALYSIS OF SLOT LEADERS ELECTION PROCEDURE FOR POS-BASED BLOCKCHAINS WITH ON-CHAIN RANDOMNESS GENERATION

Lyudmila Kovalchuk [1,2], Dmytro Kaidalov [1],
Mariia Rodinko [1,3], Roman Oliynykov [1,3]
[1] IOHK, Singapore
[2] National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
[3] V.N. Karazin Kharkiv National University, Kharkiv, Ukraine

**Abstract**

The paper presents two versions of grinding attack on slot leaders election procedure for PoS and DPoS consensus protocols with on-chain randomness generation, in which an adversary tries to increase his ratio of blocks with commitments or blocks in the whole epoch. It is shown that even in the best case for the adversary he needs at least around 40% of the whole stake to succeed in this attack. The adversary with a stake ratio about 44% can easily capture half of all blocks in the epoch with probability close to 1.

**Keywords:** blockchain, grinding attack, Proof-of-Stake, consensus protocol.

## 1 Introduction

Nowadays, decentralized cryptocurrency blockchains are based on Proof-of-Stake (PoS) consensus protocol [1, 2]. Sometimes PoS consensus protocol may be enhanced with additional block confirmation procedures to decrease the probability of double spend attack and splitting attack. In such protocol there are at least two types of participants: slot leaders (or, in some blockchains, bakers), who create blocks, and endorsers who agree on blocks. To become a slot leader or an endorser, it is necessary to have some minimum stake, which is different for different blockchains. If a user does not have enough coins to participate in the protocol, he can use delegation, if consensus protocol allows this (so-called Delegated Proof-of-Stake, DPoS).

In PoS-based blockchains, blocks are grouped into cycles, which are often called epochs. The list of slot leaders and endorsers for current epoch is deter-

mined in some previous epoch by a follow-the-satoshi strategy starting from a random seed computed from information already found on the blockchain.

A grinding attack [3] affects PoS systems by exploiting the lack of randomness in the slot leader election procedure. In this case, a participant can manipulate election process and essentially increase his chance to be elected as a block producer. In particular, grinding attacks on PoS protocols are considered in [4], where it is proposed Interactive Proof-of-Stake protocol with increased resistance to such attacks. Interesting results on grinding attacks are also presented in [5].

**Our results.** In this paper we formulate simple and generalised versions of grinding attack on the procedure of slot leaders and/or endorsers election for PoS and DPoS protocols, which use shared randomness in some incorrect way. We obtained formulas for probabilities of both versions of this attack and calculated corresponding numerical results for different stake ratio of adversary. The numerical results obtained for some fixed parameters (such as epoch length and number of blocks with commitments in one epoch) show that to get a half or more blocks in a whole epoch, the adversary needs to have stake ratio not less than $p = 0.44$ to implement a simple version of attack, and not less than $p = 0.4$ to implement its generalised version with high probability.

## 2 Description of slot leaders' election and grinding attack

In this section we give a general description of the procedure of slot leaders' election and an informal description of the grinding attack on this procedure. The formal description of the attack will be given in the next section.

As it was mentioned, the whole process of block generation in PoS-based blockchains is divided into epochs. Each epoch with the number $i$ is associated with a random seed which is used for a random selection of a roll snapshot from epoch with the number $i - 2$ and the rolls in this snapshot. The selected rolls determine the mining and endorsing rights in the epoch $i +$ PRESERVED_EPOCHS (a branch whose fork point is in an epoch more than PRESERVED_EPOCHS in the past is not accepted).

For simplicity we suppose that each epoch has BLOCKS_PER_EPOCH = 4096 blocks and the random seed for the epoch with the number $i$ is a 256-bit number generated at the very end of the epoch with the number $i - 1$ from nonces to which delegates commit during the epoch with the number $i - 2$. We also assume that one out of every BLOCKS_PER_COMMITMENT = 32 blocks can contain a commitment. So, there are at most BLOCKS_PER_EPOCH / BLOCKS_PER_COMMITMENT = 128 commitments in each epoch. A commitment is the hash of a nonce that is generated by the slot leader who produces the block and is included into the block header. The committed nonce must be revealed by the original slot leader during the epoch with the number $i-1$ under penalty of forfeiting the rewards and fees of the block that included the com-

mitment. The associated security deposit is not forfeited. A nonce revelation is an operation, and multiple nonce revelations can thus be included into a block. A slot leader receives some SEED_NONCE_REVELATION_TIP reward for including a revelation. Revelations are free operations which do not compete with transactions for block space. Up to MAX_REVELATIONS_PER_BLOCK = 32 revelations can be contained in any given block.

Thus, (BLOCKS_PER_EPOCH / MAX_REVELATIONS_PER_BLOCK) / BLOCKS_PER_COMMITMENT = 4 blocks in an epoch are sufficient to include all revelations. The seed for the epoch with the number $i$ is obtained as follows: the seed of the epoch with the number $i-1$ is hashed with a constant and then with each nonce revealed in the epoch with the number $i-1$.

The grinding attack we propose is based just on this slot leaders' election procedure. Note that the endorsers' election procedure is very similar, so the attack described bellow is also suitable for endorsers' election.

Let an attacker that controls $p$-fraction of a stake for some significant minority (say $p = 0.1$) trying to grind on the nonce for the epoch $i$ do the following.

- In the epoch with the number $i-2$, the average number of commitment-containing blocks to be attributed to the adversary is $128p$ (i.e., he is elected as the highest-priority slot leader for these blocks). In each of these blocks, the adversary includes commitments into random nonces just as the protocol prescribes.

- In the epoch with the number $i-1$, slot leaders of commitment-containing blocks from the epoch with the number $i-2$ are supposed to open their commitments and publish the underlying nonces that they committed to. Assuming that all other nonce-creators from the epoch with the number $i-2$ are honest, the adversary will see their openings (and hence their nonces) soon after the start of epoch with the number $i-1$. Now he can decide which of his commitments are to be opened: if he created around $128p$ commitments in the epoch with the number $i-2$, he has around $2^{128p}$ possibilities to choose from (for example, in the 10% example this is around $2^{13}$ ). For each of these possibilities (as long as his computational capacities allow), the adversary computes the resulting randomness seed for the epoch with the number $i$ + PRESERVED_EPOCHS, and chooses the possibility that gives her the most highest-priority baking positions in that epoch.

- The adversary waits until the epoch with the number $i$ + PRESERVED_EPOCHS and uses the disproportional block-creating rights, either for executing the grinding attack again (just stronger), or for getting disproportional rewards for baking, or for some other attack like double-spending.

# 3 Probabilities of two variants of grinding attack

In this section, we consider two variants of a grinding attack. Both of them are a two-steps attack and are different only at the second step.

**Step 1.** On this step, the adversary waits for opening of all other commitments and then decides what variant of grinding is more profitable for him at the second step: to maximize the number of his blocks with commitments (purposing to increase the number of grinding trials at the second step), or to maximize the number of his blocks in the corresponding epoch.

**Step 2, variant 1.** If it is more profitable to increase his ratio in blocks with commitments, he opens corresponding commitments and uses grinding to maximize the number of nonce commitment blocks. (It may help him to increase the number of grinding trials at the following step, if he decides to continue the process).

**Step 2, variant 2.** If it is more profitable to increase his ratio in all blocks in the epoch, he opens corresponding commitments and uses grinding to maximize the number of his slots in the whole epoch.

**Theorem 1.**

Let in the epoch number $i + \text{PRESERVED\_EPOCHS}$ the adversary tries to increase the number of his commitment blocks or blocks in the whole epoch, using his commitments from the epoch number $i - 2$.

Then the probability $P\big(B(X,l)\big)$ of the event

$$B(X,l) = \{\text{in the epoch number } i + \text{PRESERVED\_EPOCHS}$$

$$\text{adversary gets } l \text{ out of } X \text{ blocks}\}$$

is equal to

$$P\big(B(X,l)\big) = \sum_{k=0}^{n} \left(1 - \Big(1 - P\big(A(X,l)\big)\Big)^{2^k}\right) \times \left(\begin{array}{c} k \\ X \end{array}\right) p^k q^{n-k}, \qquad (1)$$

where $p$ is the adversary's stake ratio, $q$ is the stake ratio of honest participants, $X \in \{n, N\}$ and

$$P\big(A(X,l)\big) = \sum_{k=l}^{X} \left(\begin{array}{c} X \\ k \end{array}\right) p^k q^{X-k}.$$

Substituting $N$ or $n$ instead of $X$ into (1), we get two formulas for probabilities that the adversary with the stake ratio $p$ managed to get not less than $l$ blocks in whole epoch or not less than $l$ commitment blocks, respectively, where $0 \le l \le X$.

# 4 Numerical results

Here we adduce two tables with numerical results obtained according to formula (1) for $X = n = 128$ (Table 1) and $X = N = 4096$ (Table 2).

Table 1: Probability that an adversary with a stake ratio $p$ managed to get $l$ or more commitment blocks in the epoch $i+$PRESERVED_EPOCHS, using his commitments from epoch $i-2$ (for $X = n = 128$)

| | $l$ | | | | |
|---|---|---|---|---|---|
| $p$ | $0.1n = 12$ | $0.15n = 19$ | $0.2n = 25$ | $0.25n = 32$ | $0.3n = 44$ |
| 0.1 | 0.999994 | 0.996895 | 0.810652 | 0.053589 | $9.54\text{E}-05$ |
| 0.15 | 1 | 1 | 0.999995 | 0.996898 | 0.831635 |
| 0.2 | 1 | 1 | 1 | 1 | 0.999995 |
| 0.25 | 1 | 1 | 1 | 1 | 1 |
| 0.3 | 1 | 1 | 1 | 1 | 1 |
| 0.35 | 1 | 1 | 1 | 1 | 1 |
| 0.4 | 1 | 1 | 1 | 1 | 1 |
| 0.45 | 1 | 1 | 1 | 1 | 1 |
| 0.5 | 1 | 1 | 1 | 1 | 1 |
| | $l$ | | | | |
| $p$ | $0.35n = 44$ | $0.4n = 51$ | $0.45n = 57$ | $0.5n = 64$ | |
| 0.1 | $1.57\text{E}-08$ | $5.2\text{E}-16$ | $6.2\text{E}-21$ | $2.7\text{E}-27$ | |
| 0.15 | 0.157741 | 0.000369 | $9.12\text{E}-08$ | $5.2\text{E}-19$ | |
| 0.2 | 0.998135 | 0.80569 | 0.144884 | 0.000337 | |
| 0.25 | 1 | 0.999989 | 0.995971 | 0.712103 | |
| 0.3 | 1 | 1 | 1 | 0.999953 | |
| 0.35 | 1 | 1 | 1 | 1 | |
| 0.4 | 1 | 1 | 1 | 1 | |
| 0.45 | 1 | 1 | 1 | 1 | |
| 0.5 | 1 | 1 | 1 | 1 | |

According to Table 2, we can conclude that to get not less than a half of blocks in a whole epoch in simple two-step grinding attack adversary should have stake ratio about 0.44. With smaller stake rate such event has negligible probability.

# 5 A few words about generalisation of grinding attack

Now let us get back to the generalization of the attack mentioned in Section 3 .

This generalization is as follows. After Step 1, the attacker makes several iterations corresponding to variant 1 of Step 2, gradually increasing his share among the blocks with commitments. Having increased it to the desired value, he goes to variant 2 of Step 2 and tries to get at least half of all the blocks of the next epoch. Is this generalised attack significantly more effective than the simpler one, discussed earlier? And does it make sense to do many iterations aimed at increasing the number of blocks with commitments? Will it help the

Table 2: Probability that an adversary with a stake ratio $p$ managed to get $l$ or more blocks in the whole epoch $i$ + PRESERVED_EPOCHS, using his commitments from epoch $i-2$ ($X = N = 4096$)

| | $l$ | | | | |
|---|---|---|---|---|---|
| $p$ | $0.1n = 409$ | $0.15n = 614$ | $0.2n = 819$ | $0.25n = 1024$ | $0.3n = 1228$ |
| 0.1 | 0.999986 | 6.25E − 20 | 1.8E − 77 | 8.4E − 163 | 3.6E − 272 |
| 0.15 | 1 | 1 | 3.13E − 14 | 1.1E − 58 | 1.1E − 127 |
| 0.2 | 1 | 1 | 1 | 0.000048 | 5.5E − 50 |
| 0.25 | 1 | 1 | 1 | 1 | 0.0508 |
| 0.3 | 1 | 1 | 1 | 1 | 1 |
| 0.35 | 1 | 1 | 1 | 1 | 1 |
| 0.4 | 1 | 1 | 1 | 1 | 1 |
| 0.45 | 1 | 1 | 1 | 1 | 1 |
| 0.5 | 1 | 1 | 1 | 1 | 1 |
| | $l$ | | | | |
| $p$ | $0.35n = 1433$ | $0.4n = 1638$ | $0.45n = 1843$ | $0.5n = 2048$ | |
| 0.1 | 3.6E − 403 | 1.4E − 553 | 1.4E − 721 | 1.4E − 908 | |
| 0.15 | 3.2E − 217 | 3.2E − 326 | 3.2E − 454 | 8.2E − 600 | |
| 0.2 | 1.3E − 108 | 2.8E − 187 | 5.7E − 285 | 5.7E − 399 | |
| 0.25 | 7.4E − 46 | 1.3E − 98 | 2.2E − 170 | 3.3E − 260 | |
| 0.3 | 0.58 | 3.5E − 44 | 4.8E − 94 | 6.3E − 161 | |
| 0.35 | 1 | 0.962 | 6.2E − 45 | 2.8E − 92 | |
| 0.4 | 1 | 1 | 0.999154 | 8.6E − 47 | |
| 0.41 | 1 | 1 | 1 | 1.8E − 40 | |
| 0.42 | 1 | 1 | 1 | 7.9E − 34 | |
| 0.43 | 1 | 1 | 1 | 5.08E − 29 | |
| 0.44 | 1 | 1 | 1 | 0.9589 | |
| 0.45 | 1 | 1 | 1 | 0.999993 | |
| 0.5 | 1 | 1 | 1 | 1 | |

adversary to get half or more blocks in a whole epoch?

Let us try to answer these questions. Suppose that the attacker, as a result of the iterative execution of variant 1 of Step 2, managed to obtain all 128 blocks with commitments. Also make an assumption in favour of the attacker, and suppose that his computational abilities are sufficient to enumerate all $2^{128}$ options for opening commitments (although this is hardly possible without a quantum computer). We will not build anything like Tables 1 and 2 with large volume of calculations, but only estimate the probability $P\left(B\left(4096, 2048, 2^{128}\right)\right)$ that an attacker with a stake ratio $p$ will be able to get more than half of all blocks of the corresponding epoch, if in the previous epoch he received all the blocks with commitments. Also we estimate the minimal stake ratio for which such probability is significant.

According to our previous results,

$$P\left(B\left(4096, 2048, 2^{128}\right)\right) = 1 - \left(1 - P\left(A\left(4096, 2048\right)\right)\right)^{2^{128}} \tag{2}$$

where

$$P(A(4096, 2048)) = \sum_{k=2048}^{4096} \left( \begin{array}{c} 4096 \\ k \end{array} \right) p^k q^{4096-k}. \tag{3}$$

The problem is to calculate (2) and (3) with sufficient accuracy.

First of all, note that $2^{128} \approx 10^{38,8} < 10^{39}$. Then, if $P(A(4096, 2048)) < 10^{-41}$, we can approximate (2) as

$$P\left(B\left(4096, 2048, 2^{128}\right)\right) \approx 10^{39} \cdot P(A(4096, 2048)) \tag{4}$$

where calculation error is not larger than $\left(10^{39} \cdot P(A(4096, 2048))\right)^2 < 10^{-4}$.

Next, note that $P(A(4096, 2048))$ increases with an increasing stake ratio $p$. As for $p = 0.39$ we get $P(A(4096, 2048)) \approx 2.6 \cdot 10^{-46}$, then we can use approximation (2) for all stakes which are not large than 0.39.

Using (2) for $p = 0.39$, we get negligible small probability

$$P\left(B\left(4096, 2048, 2^{128}\right)\right) \approx 10^{39} \cdot 2.6 \cdot 10^{-46} = 2.6 \cdot 10^{-7}$$

which allows us to conclude that for smaller stake ratios probabilities of such events will also be negligible.

For $p = 0.4$ we get

$$P(A(4096, 2048)) \approx 1.8 \cdot 10^{-38},$$

so in this case we cannot apply approximation (4).

Calculating expression in right part of (2) directly for $p = 0.4$ we get

$$P\left(B\left(4096, 2048, 2^{128}\right)\right) \approx 0.99999999999999,$$

which is indistinguishable from 1.

Based on these numerical results, we can conclude that a generalisation of grinding attack, aimed to obtain a half or more blocks in a whole epoch, doesn't work when adversary's stake ratio is not large than $p = 0.39$, even in the case if he was lucky to get all commitment blocks in some epoch.

# 6 Conclusions

We proposed and analyzed two versions of grinding attack on slot leaders election procedure in PoS and DPoS protocols, in which an adversary tries to increase his ratio of blocks with commitments or ratio of blocks in the whole epoch. We show that even in the best case for the adversary he needs at least around 40% of the whole stake to succeed in this attack. But on the other hand, the adversary with a stake ratio about 44% can easily capture half of all blocks in the epoch with probability close to 1, having significantly smaller stake ratio.

# 7 Acknowledgements

We thank Peter Gaži and Prof. Alexander Russell for proposing the idea and further discussions helped to improve the results presented.

# References


[1] Mikolaj Karpinski, Lyudmila Kovalchuk, Roman Kochan, Roman Oliynykov, Mariia Rodinko, and Lukasz Wieclaw. Blockchain technologies: Probability of double-spend attack on a proof-of-stake consensus. *Sensors*, 21(19):6408, 2021.

[2] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual international cryptology conference*, pages 357–388. Springer, 2017.

[3] Evangelos Deirmentzoglou, Georgios Papakyriakopoulos, and Constantinos Patsakis. A survey on long-range attacks for proof of stake protocols. *IEEE Access*, 7:28712–28725, 2019.

[4] Alexander Chepurnoy. Interactive proof-of-stake. *arXiv preprint arXiv: 1601.00275*, 2016.

[5] Sarah Azouvi and Daniele Cappelletti. Private attacks in longest chain proof-of-stake protocols with single secret leader elections. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, pages 170–182, 2021.