Proof-of-Stake at Stake: Predatory, Destructive Attack on PoS Cryptocurrencies

Suhyeon Lee
CIST (Center for Information Security and Technologies)
School of Cybersecurity
Korea University
orion-alpha@korea.ac.kr

Seungjoo Kim
CIST (Center for Information Security and Technologies)
School of Cybersecurity
Korea University
skim71@korea.ac.kr

ABSTRACT

There have been several 51% attacks on Proof-of-Work (PoW) blockchains recently, including Verge and GameCredits, but the most noteworthy has been the attack that saw hackers make off with up to $18 million after a successful double-spend was executed on the Bitcoin Gold network. For this reason, the Proof-of-Stake (PoS) algorithm, which already has advantages of energy efficiency and throughput, is attracting attention as an alternative to the PoW algorithm. With a PoS, the attacker needs to obtain 51% of the cryptocurrency to carry out a 51% attack. But unlike PoW, the attacker in a PoS system is highly discouraged from launching a 51% attack because he would have to risk losing his entire stake amount to do so. Moreover, even if a 51% attack succeeds, the value of PoS-based cryptocurrency will fall, and the attacker with the most stake will eventually lose the most. In this paper, we propose a predatory, destructive attack on PoS cryptocurrencies. The attacker destroys the PoS cryptocurrency system. Then, using the significant depreciation of cryptocurrency, our method can make a profit from a 51% attack on the PoS cryptocurrencies using the traditional stock market's *short selling* (or *shorting*) concept. Our findings are an example to show that the conventional myth that "a destructive attack that destroys the blockchain ecosystem totally will not occur because it is fundamentally unprofitable to the attacker itself" may be wrong.

CCS CONCEPTS

• **Security and privacy → Distributed systems security**.

KEYWORDS

blockchain, cryptocurrency, Proof-of-Stake, short selling, shorting, security, 51% attack, Ethereum

ACM Reference Format:
Suhyeon Lee and Seungjoo Kim. 2020. Proof-of-Stake at Stake: Predatory, Destructive Attack on PoS Cryptocurrencies. In *3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2020), September 25, 2020, London, United Kingdom.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3410699.3413791

CryBlock 2020, September 25, 2020, London, United Kingdom

ACM ISBN 978-1-4503-8079-9/20/09…$15.00
https://doi.org/10.1145/3410699.3413791

1 INTRODUCTION

The 51% attack controlling more than half of the total hashing power of a network is a technique which intends to fork a Proof-of-Work (PoW) blockchain in order to conduct double-spending. Due to the immense attacking cost to perform the 51% attack, it was considered very unlikely for a long period. However, in recent times, the attack has befallen at a frequent pace, costing millions of dollars to various PoW-based cryptocurrencies such as Verge, GameCredits, Bitcoin Gold, and so on.

For this reason, the Proof-of-Stake (PoS) algorithm, which already has advantages of energy efficiency and throughput, is attracting attention as an alternative to the PoW algorithm. PoS was first created in 2012 by two developers called Scott Nadal and Sunny King, and the first-ever blockchain project to use the PoS model was Peercoin. PoS is a category of consensus algorithms for public blockchains that depend on a validator's economic stake in the network. While PoW rewards its miner for solving complex equations, in PoS-based public blockchains (e.g. Ethereum's Casper implementation), a set of validators take turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of their deposit (i.e. stake).

With a PoS, the attacker needs to obtain 51% of the cryptocurrency to carry out a 51% attack. But unlike PoW, an attacker in a PoS system is highly discouraged from launching 51% attack because he would have to risk of depreciation of his entire stake amount to do so. In comparison, a bad actor in a PoW system will not lose their expensive mining equipment if he launches a 51% attack. Moreover, even if a 51% attack succeeds, the value of PoS-based cryptocurrency will fall, and the attacker with the most stake will eventually lose the most. For these reasons, those who attempt to attack 51% of the PoS blockchain will not be easily motivated. In "A Proof of Stake Design Philosophy [2]", Vitalik Buterin described these characteristics as the following:

> *"The one-sentence philosophy of proof of stake is thus not security comes from burning energy, but rather security comes from putting up economic value-at-loss."*

In this paper, we will analyze the 51% attack on the PoS blockchain more precisely. Through this, we will show that even 51% of attacks on PoS blockchain can fully benefit the attacker, and if the attack is not properly handled, the entire PoS blockchain ecosystem may be destroyed. Predatory shorting attacks in the conventional finance area are studied in Liu [8], Brunnermeier et al. [1]. Their studies showed how shorting makes a failure in financial institutions by aggravating uncertainty. Not like them, our attack model

makes PoS cryptocurrencies failure by undermining the system itself. Our contributions are summarized as the following:

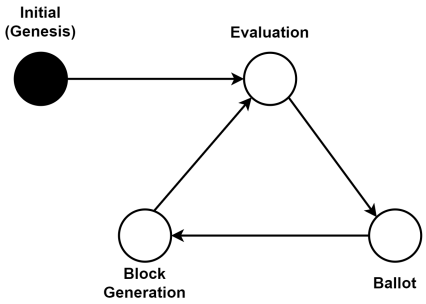
- To the best of our knowledge, this is the first sophisticated analysis on the profitability of the 51% attacker in PoS environment.
- We propose a new attacker model, "*short selling attack*" or "*shorting attack*", against PoS-based cryptocurrency using the traditional stock market's *short selling* (or *shorting*) concept.

This paper is organized as follows. We introduce a simple PoS-based cryptocurrency model in section 2. Based on this model, we propose a profitable 51% attacker model using shorting in section 3, and discuss the limitations and the future directions of our work in section 4. The conclusions are shown in section 5.

2 POS MODEL

In this section, we show our PoS cryptocurrency model. We call our cryptocurrency model as '*SimPoS*' and coin of it as '*SimPoS coin*' if we need in this paper. It is modeled by referring PPCoin [6], Ethereum [9] and Ouroboros [5], and implements the basic philosophy of PoS that stakeholders have the right to produce blocks in proportion to staking. According to this philosophy, one block generator is elected proportionally to the amount of stake for each epoch. For simplicity, the cryptocurrency creates six blocks during an epoch. It does not have the policy to punish or slash rule breakers' stake. Thus, it is a pure implementation of Proof-of-Stake. SimPoS comprises four steps which are genesis, stake evaluation, ballot, and block generation as the following description. And it is also illustrated as a state machine in Figure 1. For reference, in our model, there is no punishment to the block generator's stake even if it does not behave correctly.

Figure 1: PoS Model



Step 1. (Genesis) The genesis block is created. And the first block creates the first coins to the first address.

Step 2. (Stake Evaluation) The total staking score is updated for every participant. The staked coins cannot be spent for three months, and valid for the ballot process (Step 3) for three months.

Step 3. (Ballot) Based on the previous stake evaluation, the next block generator during one epoch is elected by the probability proportional to the participants' stake.

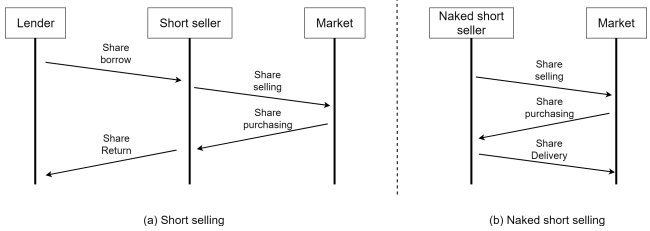
Step 4. (Block Generation) In this step, a participant who is elected as a block generator in the previous ballot process generates six blocks. The new six blocks contain a mathematical signature of the block generator so that the network can check their validity.

3 SHORT SELLING ATTACK

In this section, we introduce the traditional stock market's short selling (or shorting) concept, which is a method to bet on depreciation. Then, we propose a new predatory, destructive 51% attack, named 'short selling (or shorting) attack', in PoS cryptocurrencies.

3.1 Short Selling Concept

Figure 2: Short selling cases



In general cases, if a person owns some stock and its value falls, he will have to lose money. However, there are several ways to benefit from this downside. We can handle the risk of decline of prices by 'short selling' and 'derivatives', including 'futures' and 'options'. For the convenience of explanation, this paper describes only the short selling and proposes an attack model using short selling.

Definition 1. (Short Selling) The short selling (as known as a short sale, short, or shorting) is a fairly simple concept — an investor borrows a stock, sells the stock, and then buys the stock back to return it to the lender. Short sellers are betting that the stock they sell will drop in price. If the stock does drop after selling, the short seller buys it back at a lower price and returns it to the lender. The difference between the selling price and the buying price is the profit.

According to the short selling strategy of Definition 1, the seller sells the borrowed asset at the market price. Then, the seller should repurchase the asset to the lender as much as the seller borrowed for some time. During the time interval, the market price of the asset changes. If the market price of the asset decreased during the time interval, the short seller profits. Conversely, if not, the short selling results in a loss. The maximum profit of the short selling is the market price at the time the seller borrows the asset. The maximum loss of short selling is theoretically unlimited. In general,

the market requires a short seller to make a deposit to cover the loss.

There are two kinds of short selling. One is 'short selling', and the other is 'naked short selling'. The short selling is what we already described above. In the naked short selling, the seller sells an asset without borrowing an asset. After a set time, the seller should deliver the asset share to the market. The naked short selling is regulated in some markets.

Like the traditional stock market, some cryptocurrency exchanges, like Bitmex, also provide the short selling function to clients. Furthermore, some exchanges offer a strong feature, margin trading, to maximize gains and losses of participants. Margin trading is a method to trade assets using funds borrowed by a third party. If a person uses margin trading in short selling, he can make multiplied effects of short selling.

Table 1 shows a list of cryptocurrency exchanges that provide their features and margin trading capability. In the table, *Volume* indicates the volume of traded coins in 24 hours, *Derivatives* indicates if an exchange provides any kinds of derivatives including options and futures, and *Margin Trading* indicates how much margin leverage an exchange provides.

Notice that this table does not list all active exchanges that support short selling, and we did not test transactions in them to make sure they actually function. We got data on the listed exchanges in October 2019 by referring to the Coin Market Capital and CoinGecko. For reference, CoinOne once offered public sales and margin trading on the Korean bourse, but that function was suspended due to the legal issues of Korea.

Based on the environment of exchanges and simplicity, we assume the 51% attacker uses a cryptocurrency exchange which provides the naked short selling function, and it has big enough asset supply.

Table 1: Cryptocurrency exchanges with short selling

Exchange	Volume ($)	Derivatives	Margin Trading
BitMex	886,007,632	✓	up to 100x
Bybit	716,387,848	✓	up to 100x
Coinfloor	347,269,026		up to 100x
PrimeXBT	90,115,864	✓	up to 100x
Kraken	33,180,001		up to 5x
HitBTC	14,066,926		up to 3x
Poloniex	9,940,037		up to 100x
bitFlyer	9,141,821	✓	up to 100x
BitMax	5,233,272	✓	up to 10x
Bibox	2,225,506		up to 50x
OKCoin	634,708	✓	up to 100x

3.2 A Predatory, Destructive But Profitable 51% Attack On PoS Cryptocurrencies

We name our new attack strategy "short selling (or shorting) attack". It is based on two ideas. The first is that shorting makes a profit from the loss of market value. And, the second is that the ratio of staked coins to owned coins is limited because of financial liquidity. So the attacker does not need to own 51% of the total amount of coins. He only needs to own 51% of the mean staking ratio of the total amount of coins.

Definition 2. (Short Selling (or Shorting) Attack) The short selling (or shorting) attack is a kind of 51% attack in PoS-based cryptocurrencies. After achieving 51% stake, the attacker sabotages the system with any methods right after short selling a massive amount of the cryptocurrency for profit.

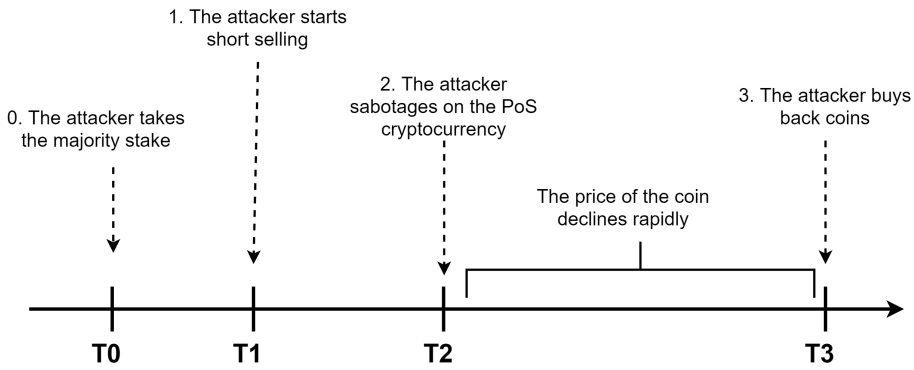
The attack strategy is three-step. Figure 3 shows attack steps with time flow, T0 - T3. The attacker's target is SimPoS which is introduced in Section 2. Before the attack, we assume that the attacker makes stakes over 51% of the total stake at time T0.

Assumption 1. The cryptocurrency system's value is on the functionality of transactions

Let the amount of the staked coins of the attacker be A.

Step 1. (Short Selling) The attacker shorts coins in a market at time T1. Let the amount of the short selling be B.

Figure 3: Attack diagram with time flow



Step 2. (Sabotage) The attacker commits sabotage to the cryptocurrency system. For simplicity, the attacker generates empty blocks continuously from time T2.

We assume the value of the cryptocurrency system is based on the functionality of decentralized cryptocurrency transactions rather than long term saving or investment. Therefore, people do not need to keep SimPoS coins in their wallets anymore. Then, the market value of SimPoS coin declines steeply. If people believe that SimPoS will not work anymore, its market value will decline to nearly zero. Let's the depreciation ratio from time T2 to T3 be Δ.

Step 3. (Buyback) At time T3, the attacker buys SimPoS coins to deliver to the market for shorted coins.

As a result, the attacker gains $\Delta \cdot (B - A)$. To be profitable, The short amount of B should be more significant than A. For reference, the attacker can gain a short amount of B not only by owning the cash corresponding to the market value of B coins but also by using the margin trading. We can see historical Δ values in the previous security accidents in Table 2. Even though we add a slashing policy removing rule breakers' coins into our model, the attacker model can be profitable if depreciation by the attack is big enough. Furthermore, the attacker already became the majority and generates only empty blocks. It means others' cannot stake anymore. The attacker can keep the majority stake and keep the attack until stakeholders gave up SimPoS and it results in great depreciation.

Table 2: Depreciation cases by attacks

Coin	P_{MAX} date/price(USD)	P_{DAM} date/price(USD)	Δ
ETH	01/17/2016 13:19:22	June 16 2016 13:19:22	34%
	21.49	14.29	
ETC	01/07/2019 09:04:03	January 08 2019 13:19:22	11%
	5.50	4.92	
BTG	05/24/2018 14:34:17	May 25 2018 14:34:17	1%
	47.62	47.18	
VTC	06/12/2018 14:49:00	December 07 2018 14:49:00	25%
	0.316917	0.238420	
XVG	04/04/2018 04:34:04	April 05 2018 04:34:04	21%
	0.075580	0.059703	

4 DISCUSSION

4.1 Short Selling Can Be Combined

Our attack is not only available by the short selling but also by futures and options. The futures, options, and swaps discussed here are just the classic products, called plain vanilla, of derivatives. In theory, almost infinite forms of derivatives may exist. We are not yet sure whether the cryptocurrency will remain safe even among these various derivatives. All we can say is that cryptocurrencies are secure only under very limited conditions. In economics, it is called '*Ceteris Paribus*'. In Korea, Coinone, one of the biggest cryptocurrency exchanges, has been abolished the short selling and the margin trading system due to state policy. In this case, people should consider the exchange level to restrict such derivatives, but nobody knows whether these restrictions are in the right direction for the decentralized cryptocurrencies.

4.2 Social Cost & Punishment

Social costs and punishment policies can cause disadvantages to our method. In this paper, our work's scope was limited to the economic costs in the simple PoS model. At first, Buterin's optimistic outlook was based on the perspective that the 51% attack would include social costs as well as economic costs. For example, the situation that blockchain nodes revert the context before 51% attacks can happen. Though it is not regulated in the consensus mechanism, it will be a cost to the attacker. Secondly, PoS is getting robust to attacks with punishment policies [3, 4]. Blockchain participants can make rules that regulates nullification of all of the attacker-related assets (beyond slashing) and even the restriction of attacker-related funds on the exchange. Then, it would decrease the revenue of our attack methodology. These two perspectives should be included in future work to construct a comprehensive model.

5 CONCLUSIONS

The rationale behind PoS is that entities who hold a stake in the system are well-suited to maintain its security since their stake will diminish in value when the security of the system erodes. Thus, we have believed that a 51% attack that does not benefit anyone, including attackers, will not happen on the PoS blockchain until now. In this paper, however, we showed that a 51% attack on the PoS blockchain could benefit the attacker sufficiently by using short selling. Our findings will be an example to show that the conventional myth that "a destructive attack that wrecks the blockchain ecosystem will not occur because it is fundamentally unprofitable to the attacker itself" may be wrong.

ACKNOWLEDGMENTS

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2020-2015-0-00403)supervised by the IITP(Institute for Information &communications Technology Planning &Evaluation). We would like to gratefully acknowledge comments and encouragement from Donghwan Lee, the senior researcher of Agency for Defense Development (ADD).

REFERENCES

[1] Markus K Brunnermeier and Martin Oehmke. 2014. Predatory short selling. *Review of Finance* 18, 6 (2014), 2153–2195.
[2] Vitalik Buterin. 2016. A Proof of Stake Design Philosophy. https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51. [Online; accessed 10-July-2020].
[3] Vitalik Buterin. 2020. Immediate message-driven GHOST as FFG fork choice rule. https://ethresear.ch/t/immediate-message-driven-ghost-as-ffg-fork-choice-rule/2561. [Online; accessed 10-July-2020].
[4] NKB Group. 2020. Ethereum releases Casper v0.1: A short description for validators. https://medium.com/@theNKBGroup/ethereum-releases-casper-v0-1-a-short-description-for-validators-3e0a7676d286. [Online; accessed 10-July-2020].
[5] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. 2017. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*. Springer, 357–388.
[6] Sunny King and Scott Nadal. 2012. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August* 19 (2012).
[7] Suhyeon Lee and Seungjoo Kim. 2020. Short Selling Attack: A Self-Destructive But Profitable 51% Attack On PoS Blockchains. Cryptology ePrint Archive, Report 2020/019. https://eprint.iacr.org/2020/019.

[8] Xuewen Liu. 2010. *Predatory short-selling and self-fulfilling crises.* Technical Report. Working paper, HKUST.

[9] Ethereum wiki contributors. 2020. Proof of Stake Frequently Asked Questions. https://eth.wiki/en/concepts/proof-of-stake-faqs. [Online; accessed 10-July-2020].