Short Selling Attack: A Self-Destructive But Profitable 51% Attack On PoS Blockchains

Suhyeon Lee and Seungjoo Kim
CIST (Center for Information Security Technologies), Korea University, Korea

***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, attacker in a PoS system is highly discouraged from launching 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 try to derive the results that go against these conventional myths. Despite of the significant depreciation of cryptocurrency, our method can make a profit from a 51% attack on the PoS blockchains 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.**

***Index Terms*—Blockchain, Cryptocurrency, Proof-of-Stake, 51% attack, Ethereum**

I. 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, 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, bad actor in a PoW system will not lose their expensive mining equipment if he launch 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 follows:

> *"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. Our contributions are summarized as follows:

- 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, "SimPoS", in section II. Based on this model, we propose a profitable 51% attacker model using shorting in section III, and discuss the limitations and the future directions of our work in section IV. The conclusions are shown in section V.

II. Our PoS Model

In this section, we introduce a cryptocurrency model for study. Our cryptocurrency model works with PoS consensus mechanism.

A. *SimPoS*

Before the analysis, we define our PoS model first. We name our cryptocurrency model as '*SimPoS*' and coin of it as '*SimPoS coin*'. It is modeled by referring PPCoin [4], Ethereum [1] and Ouroboros [3], 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, SimPoS creates six blocks during an epoch. It does not have policy to punish or slash rule breakers' stake. Thus, it is a pure implementation of Proof-of-Stake. SimPoS comprises of four steps which are genesis, stake evaluation, ballot, block generation.

Step 1. (Genesis) The genesis block is created.

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 for three months.

Step 3. (Block Generator Election) Based on the previous stake evaluation, the next block generator is elected by the probability proportional to participants' stake.

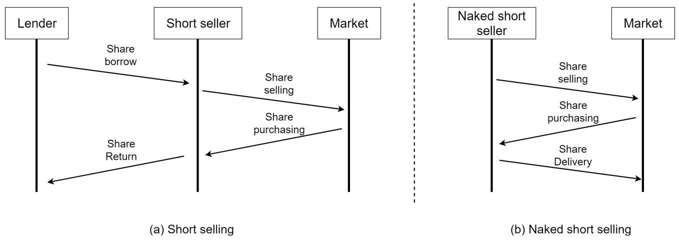
Step 4. (Block Generation) In this step, a participant who is elected as a block generator in the previous election step generates six blocks. New blocks contain a mathematical signature of the block generator so that the network can check their validity. For simplicity, in our model, there is no way to punish the block generator's stock even if it does not behave correctly.

III. 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 profitable 51% attack, called 'short selling (or shorting) attack', in a PoS cryptocurrency environment.

A. *Short Selling Concept*

Figure 1: Short selling cases



(a) Short selling

(b) Naked short selling

In the usual case, if a person owns Bitcoin 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 short selling attack model.

Definition 1. (Short Selling) The short selling (as known as a short sale, short, or shorting) is the sale of an asset which the seller has borrowed with anticipation on declines of the price of the asset.

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 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. The 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 I 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. 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.

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.

B. *A Self-Destructive But Profitable 51% Attack On PoS Blockchains*

Our new strategy is named "short selling (or shorting) attack". It is based on two ideas. The first is that shorting

Table I: 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

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 a liquidity problem. So the 51% attacker does not need to own 51% of the total amount of coins. He just 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 cryptocurrency. After achieving 51% stake, the attacker sabotages the system with any methods right after short selling a massive amount of the cryptocurrency.

The attack strategy consists of three-step. Before the attack, the attacker makes the stakes over 51% of the total stake. Let the amount of the staked coins of the attacker be A.

Step 1. (Short Selling) The attacker shorts SimPoS coin in a market. Let the amount of short be B.

Step 2. (Sabotage) The attacker commits sabotage to the SimPoS system as much as the attacker can do. For example, the attacker can generate several forks for every block, like trying double-spending. Alternatively, the attacker can generate blocks slowly. Then, the market value of SimPoS coin decreases as the cryptocurrency system cannot work normally. Let's the depreciation ratio be Δ.

Step 3. (Short Covering) The attacker buys SimPoS coins to deliver to the market for short covering.

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 II. Even though we add a slashing policy removing rule breakers' coins into our model, we can improve our shorting attack model with simple math. It is trivial so that we skip it here.

Table II: Depreciation cases by attacks

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

IV. Discussion

A. Short Selling Isn't Alone

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 no body knows whether these restrictions are in the right direction for decentralized cryptocurrencies.

B. Social Cost

Social costs and punishment policy can make disadvantage to our method. In this paper, the scope of our work was limited to the economic costs. On the other hand, 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. In policy, blockchain participants can make a rule 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.

V. Conclusions

The rationale behind PoS is that entities who hold 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, till now, we have believed that a 51% attack that does not benefit anyone, including attackers, will not happen on the PoS blockchain. 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 destroys the blockchain ecosystem totally will not occur because it is fundamentally unprofitable to the attacker itself" may be wrong.

References

[1] Proof of stake frequently asked questions. [Online; accessed 10-May-2019].

[2] Vitalik Buterin. A proof of stake design philosophy, 2016. [Online; accessed 10-May-2019].

[3] 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.

[4] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, 19, 2012.