Analysing Mining Machine Shutdown Price

Shange Fu
Monash University
Melbourne, Australia
shange.fu@monash.edu

Jiangshan Yu
Monash University
Melbourne, Australia
jiangshan.yu@monash.edu

Rafael Dowsley
Monash University
Melbourne, Australia
rafael.dowsley@monash.edu

Joseph Liu
Monash University
Melbourne, Australia
joseph.liu@monash.edu

***Abstract*—The security of PoW-based blockchain relies on the total amount of mining power and the ratio of mining power possessed by the honest miners. Loosely speaking, a system with higher mining power makes an attack more difficult. To incentivise miners joining the network and contributing their mining power, reward mechanisms are designed to provide economic profit to miners in exchange for their mining power.**

We identify shutdown price of mining machines as an overlooked factor that has an impact on the total amount of mining power, so the level of system security of PoW-based blockchains. This work fills this knowledge gap. We formalise the concept of shutdown price, which represents the break-even point of operating a mining machine. Once the shutdown price of a type of mining machines is reached, mining coins by using such machines is more expensive than buying coins directly in the cryptocurrency market. Therefore a rational operator would shut these machines down. This reduces the mining power in the network. However, as the variance of the coin price can be very high and the coin price may recover from the break-even point within a short time interval, the miners may not shut down the break-even triggered machine immediately or choose a partial shutdown strategy to hedge risk. We define and analyse such shutdown tolerance by applying real option theory.

We reveal that shutdown price can be influenced by several factors, including the halving event and electricity price. Attacks requiring a particular percentage of mining power, such as 51% attacks, can take this into account and explicitly incorporate the diminished mining power as a part of their strategy, which will reduce the difficulty of launching such attacks.

***Index Terms*—Proof-of-Work, Shutdown Price, Real Option, 51% Attack**

I. Introduction

Since the introduction of Bitcoin [25], proof-of-work (PoW) has been adopted by many blockchain systems to reach consensus on the global state of a blockchain in permissionless settings. In permissionless blockchains, anyone can join and leave at any time. This enables Sybil attacks [9], where an attacker creates lots of entities at insignificant cost. If reaching an agreement depends on the number of voters, such as the traditional Byzantine fault tolerant protocols [26], then the attacker can leverage these created entities to dominate the voting and control the voting result on the global state. This may lead to attacks such as double-spending [5].

In Bitcoin-like blockchains, proof-of-work addresses this issue by increasing the cost for each vote in the system. Each voter needs to prove that it has performed some computational work. The performed work, called mining, leads to non-negligible cost, including consumed electricity and computational power. The agreement is made by accepting the blockchain state with most performed work. If an attacker is able to control a majority of the mining power, then the attacker dominates the system's voting power. So, a higher total amount of mining power in the system provides a better security guarantee, as it becomes more difficult for an attacker to control a threshold ratio of mining power to launch attacks such as 51% attack [4] or selfish mining attack [11].

To incentivise miners joining the system and providing additional mining power, a reward mechanism is implemented in such blockchain systems – miners earn coins as a reward for their contributed mining power. To prove the performed work, miners in the system are required to solve a crypto puzzle. The one who successfully finds a solution to the puzzle will get some mining reward. For example, in Bitcoin, a successful miner obtains some block reward and transaction fees. The block reward is a pre-determined amount of bitcoins, which started as 50 bitcoins per block and halves every 210,000 blocks (about every four years). The recent halving event (on May 11 2020) was Bitcoin's third reward halving, where the block reward was reduced from 12.5 bitcoins to 6.25 bitcoins.

This paper identifies an overlooked factor that affects the security of Bitcoin-like blockchains. We fill the knowledge gap by introducing, defining, and analysing the *shutdown price* of mining machines. To perform mining, miners need to maintain mining machines with high mining power. The operational costs, such as paying for the consumed electricity, are relatively high as these machines consume a lot of energy. For example, the total amount of consumed energy in Bitcoin mining in a year is more than the annual consumption of many countries [28]. The shutdown price of a machine represents the break-even point where the mining reward is not enough to cover the costs of performing mining. In this case, miners would switch off the machine and leave the network to prevent further loss. This in turn reduces the total amount of mining power in the network and makes the system less secure. However, in reality, miners may not switch off the break-even triggered machines immediately due to a quick coin price recovery expectation, or some miners may even apply a partial shutdown strategy to hedge such risk. We define such phenomenon as *shutdown tolerance*, and analyse it using real option theory.

The shutdown threshold allows an easier execution of attacks as unprofitable mining rigs will leave the network, so the total amount of honest mining power is decreased, if the coin price decreases and triggers their shutdown prices.

During an attack, the attacker may increase its profit by trading *financial derivatives* as the price is likely to be affected by the attack. As in traditional financial markets, the financial derivatives of cryptocurrencies are becoming increasingly popular. Financial derivatives are contracts between two or more parties whose value is based on an agreed-upon underlying financial asset, such as coins in cryptocurrencies. Parties of a contract may gain or lose money depending on the change of the underlying financial asset price. Many factors might have an impact on financial asset price. For example, when a cryptocurrency is attacked (such as the 51% attack on Bitcoin Gold in 2018 [33]), people may lose their confidence in the cryptocurrency and the coin price might go down sharply. This unique binding between coin price and the financial gain from the derivatives may incentivise an attacker to launch attacks on existing cryptocurrencies, as the attacker can leverage the derivatives to gain extra profit from the attack.

Paper Organisation. The rest of this paper is organised as follows. Section II provides the necessary background on real option theory and its pricing model, which can be applied in decision making process of shutdown tolerance. Section III defines the shutdown price of PoW mining machines and provides an analysis on the shutdown tolerance, i.e., why some miners could choose to not shutdown machines even when their break-even point is triggered. It also discusses the factors influencing the shutdown price and their impacts. Section IV presents related work, Section V provides a discussion regarding multiple concerns and observations and Section VI concludes the paper.

Appendix A presents a summary of notations; Appendix B explains preliminaries including financial derivatives such as futures, exchange-traded fund, and options; Appendix C provides a discussion on the impact of shutdown price on blockchain security and Appendix D presents the shutdown price of mainstream BTC mining machines.

II. Options and Real Option Theory

This section presents an overview of financial derivatives. Options, especially real option theory can be applied into shutdown tolerance analysis in Section III.

A. Options

A financial derivative can be defined as a financial instrument whose value depends on (or derives from) the value of the *underlying asset* [15]. *Options* is a financial derivative instrument that is more complicated than other financial derivatives (see Appendix B for more details on financial derivatives). An options contract gives the contract holder the right to buy or sell an underlying asset on a fixed day in the future. A *call option* gives the holder the right to buy the underlying asset by a certain date for a certain price, while a *put option* corresponds to selling.

The price in the contract is known as the *exercise price* or *strike price*, the date on which the option expires in the contract is known as the *expiration date* or *maturity*. *American options* can be exercised at any time up to the expiration date, while *European options* can be exercised only on the expiration date itself. The *option premium* ϵ_o is the price for obtaining the options contract.

An options contract provides the holder with the right to buy or sell a specified quantity of an underlying asset at an exercise price on (or also before, if it is an American options) the expiration date. There has to be a clearly defined underlying asset whose value changes overtime in unpredictable ways. The contract holder can choose to exercise the option if doing so is advantageous, the contract seller is obliged to pay the relevant amount to the contract holder if the option is exercised. If there is no benefit from exercising, the holder can choose not to exercise it with the limited loss of the contract premium itself, then the seller does not need to pay anything in this case.

To see the payoffs of an options contract, let T be the expiration date, K be the strike price, S_T be the asset's price at maturity, and each options contract be worth a premium ϵ_o. The payoff to the buyer of a European call option, for example is given by

$$max(S_T - K - \epsilon_o, -\epsilon_o). \tag{1}$$

The Black–Scholes model achieved a major breakthrough in the pricing of dividend-protected European options in the limiting distribution settings, and was awarded the Nobel prize for economics in 1997. As the time interval is shortened and goes to zero, the Black-Scholes model applies when the limiting distribution is the normal distribution, and explicitly assumes that the price process is continuous and that there are no jumps in asset prices [15]. The value of a call option can be written as a function of the following variables: (1) the current value S_0 of the underlying asset; (2) the strike price K of the option; (3) life to expiration T of the option; (4) risk-less interest rate r; (5) variance σ^2 of the underlying asset. The value of a call option is given by

$$Call = S_0 N\left(d_1\right) - K e^{-rT} N\left(d_2\right) \tag{2}$$

where

$$d_1 = \frac{\ln\left(S_0/K\right) + \left(r + \sigma^2/2\right) T}{\sigma\sqrt{T}}, \tag{3}$$

$$d_2 = \frac{\ln\left(S_0/K\right) + \left(r - \sigma^2/2\right) T}{\sigma\sqrt{T}} = d_1 - \sigma\sqrt{T} \tag{4}$$

and the function $N(x)$ is the cumulative probability distribution function for a variable with a standard normal distribution.

B. Real Option Theory

Unlike ordinary options contracts, real option is an idea about searching for an elusive premium embedded in the investment. An action related to investment can be both a strategic and a financial task facing decision makers, and discounted cash flow (DCF) is the main valuation method that summarizes future cash flows as a present value with a discount rate. There can be real options neglected by the traditional DCF models that underestimate the value of

investments. At the early stages, investors can observe the market reaction and then take further decision such as: defer, alter, expand or even abandon the investment. This learning (or observing) period can give decision makers the opportunity to adjust their behavior and this is where real options comes in [8].

Real option can be applied under certain circumstances. For an option to have significant economic value, there has to be a restriction on competition in the event of the contingency. At the limit, real options are most valuable when you have exclusivity - you and only you can take advantage of the contingency. The options become less valuable as the barriers to competition become less steep.

However, when option pricing models are used to value real assets, we have to accept the fact that the estimated real option value could be imprecise or could deviate from the market price due to the difficulty of arbitrage. The Black-Scholes model is by far the most accessible tool that can give an approximation to the real option where the underlying asset can be traded in an active marketplace [2]. The market can provide observable price and volatility as inputs to option pricing models, and there is also the possibility of creating replicating portfolios.

III. Shutdown Price: Definition and Impact

This section defines the concept of shutdown price. As the coin price changes dynamically, miners may choose to delay shutting down mining machines (due to the operational cost). We model such decision making process as an option and analyse it by applying real option theory. Moreover, we discuss the factors that can influence the shutdown price, and give an analysis of the impact of the shutdown price on the security of blockchain systems.

A. Defining Shutdown Price

The *shutdown price* of a type of mining machine refers to the price threshold, where the cost for mining a coin is equivalent to purchasing a coin. If the price is lower than this threshold, then performing mining is more expensive than purchasing coins directly from the market. Keep mining in this case is considered as "purchasing" coins with a price that is higher than the market price. So, there is no incentive for the miners to keep mining and they will shutdown the mining machines to reduce the economic loss.

To calculate the revenue of mining, a miner mainly considers two types of cost, namely fixed cost and variable cost. The fixed cost is the amount of money paid to purchase a mining machine, which can be spread over a time period. The variable cost considers the ongoing cost to perform mining. In July 2019, BBC [1] reported that Bitcoin consumes about 7 gigawatts, which is 0.2% of the global energy consumption and is equivalent to the energy consumption of Switzerland. As mining hardware consumes a lot of energy, the electricity fee for operating mining machines is significant. If the economic gain from mining cannot cover the cost of mining (e.g. when the market price of a coin is low), then the miner will shutdown that type of machines due to the opportunity cost — it is more profitable to buy the coins directly in cryptocurrency market rather than spending more money to perform mining.

For simplicity, we consider the existence of epochs where miners join or leave the system only at the end of each epoch. Let $\mathcal{M}^t = [m_i^t]_{i=1}^n$ be a set of n mining machines in the network at the t-th epoch, such that the mining power of each mining machine m_i^t is h_i^t. We denote H^t as the collective mining power in the network at the t-th epoch, i.e., $H^t = \sum_{i=1}^n h_i^t$.

Let $\bar{w}_i$ be the power consumption (in kilowatt[1]) of a mining machine m_i^t and E^t be the average price of electricity (USD/KWh) at the t-th epoch. Let C be the number of coins, on average, given as a mining reward to the entire network per epoch, including all new minted coins and transaction fees. Let P^t be the average price of the coin (USD per coin) at the t-th epoch. We consider a system with ideal chain quality [14], i.e., the number of blocks created by a miner is in proportion to its mining power. Let the length (number of hours) of an epoch be l. The cost of mining for machine m_i^t is $l \cdot \bar{w}_i \cdot E^t$. Thus, the net revenue R_i^t of mining machine m_i^t at the t-th epoch is

$$R_i^t = \frac{h_i^t}{H^t} \cdot C \cdot P^t - l \cdot \bar{w}_i \cdot E^t. \tag{5}$$

When there is a break-even point for mining machine m_i^t at the t-th epoch, i.e. $R_i^t = 0$, we say the shutdown price $\bar{P}_i^t$ of the mining machine m_i^t is reached at the t-th epoch. Formally,

$$\bar{P}_i^t = \frac{l \cdot \bar{w}_i \cdot E^t \cdot H^t}{h_i^t \cdot C} + \theta, \tag{6}$$

where θ is a "shutdown tolerance" parameter to indicate extra concerns of not shutting machines down immediately when the shutdown price is met.

B. Shutdown Tolerance Analysis

Miners may not shutdown one type of machine immediately when the shutdown price is reached, due to the operational cost and possibility that the coin price may recover within a very short time period. Operation cost is a relatively overall consideration to the decision makers and it includes the labor cost for both switching off the machines and possible re-plug into the network. In practice, there can also be some operation default cost to the mining farm operators. To have a better deal in purchasing electricity, the operator may have an agreement with its utility supplier (such as an electricity retailer) on a predefined minimal amount of utility (mainly electricity) to consume each year. The operator may need to pay a fine if haven't consume enough utility as agreed. So the operator may continue mining even if the shutdown price is reached. Note that in this paper we don't consider the situation that miners choose not to shutdown to occupy a larger proportion in the new total hashrate in the upcoming difficulty adjustment as a game theoretical strategy, the reason is that the difficulty adjustment period is long (compared with a quick

[1]Watt is a measure of the energy per unit of time: 1 Watt = 1 J/s.

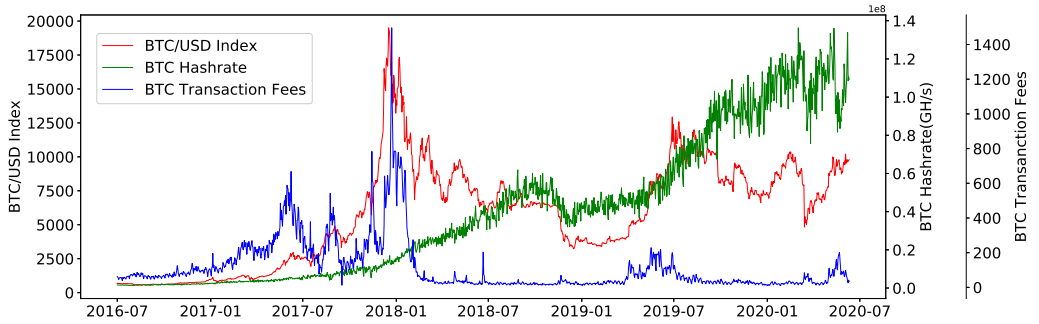

Fig. 1: BTC/USD Index, hashrate, and transaction fees. The red line represents Bitcoin price in USD, the green line represents Bitcoin network hashrate (GH/s), and the blue line represents the Bitcoin blockchain daily transactions fees in Bitcoin.

price recovery), once the coin price triggered the shutdown threshold, the machine is losing money, a rational miner will switch it off rather than stick to the next difficulty adjustment. Therefore, we denote C_{op} as the operational cost and analyse the shutdown price tolerance θ from the break-even point.

The decision making process of shutting down a machine, with the consideration of tolerance, can be modelled as the decision making for a real option, where the additional cost for making the decision is the premium on the discounted cash flow (DCF) value estimates. In this real option, a miner has the right to adjust their mining investment with the change of coin price when the break-even point is reached. If the coin price is growing up again (above the break-even point) within a short time period, then the miner decides to continue performing mining without shutting the machine down. Otherwise the miner turns machines off. This option gives the miner two significant embedded rights: learn and adjust behavior.

Consider the following scenario: When the shutdown price of a certain type of mining machines is triggered, the miner believes that the coin price would recover within one day, so he decides to keep the machines running. However, in the following 24 hours, the coin price is still decreasing and the miner keeps losing money, so he finally decides to shutdown this type of mining machine.

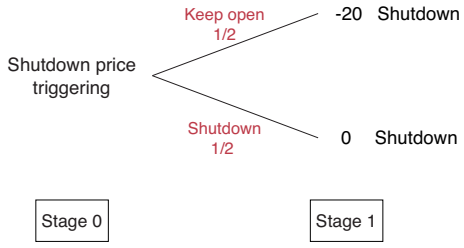

Fig. 2: A simple binomial DCF model for shutdown tolerance without considering real option.

Figure 2 and Figure 3 present the above example, with a focus on the impact of decision making process in the real option. Miners prefer not switch off machines immediately due to extra operation cost for both shutdown and re-open actions,

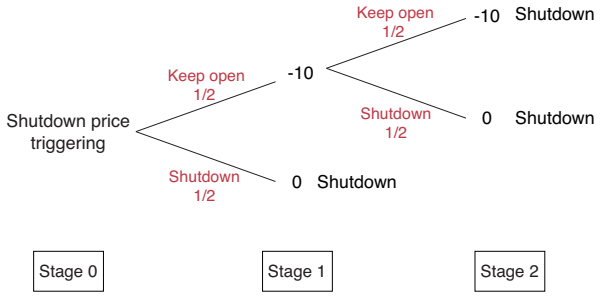

Fig. 3: Shutdown tolerance considering real option.

for simplicity, we set operation cost C_{op} for both shut down and re-open to \$0 for the actions. Therefore, if neglecting the embedded right (Figure 2), a miner may face a loss if the coin price does not recover after waiting for some time (stage 1) since the break-even point is reached (stage 0). In our example, if the miner takes shutdown action immediately, and his payoff is \$0. For a miner did not take the shutdown action, he can lose \$20 for keeping machines open if the coin price keeps falling after the 24 hours waiting time, and he should take the shutdown action after stage 1 to prevent further loss.

When considering the embedded right (Figure 3), the miner has the opportunity to observe the market from stage 0 to stage 1 as the 'early' stage by segregating the 'waiting time', and adjusts his behaviour from stage 1 to stage 2. For the same settings (wait for 24 hours in total, and coin price is decreasing), the miner can have a final payoff for \$0 as if he takes the shutdown action at stage 0. He will lose \$10 at stage 1 if not shutdown for the early stage (e.g., 12 hours), and he can choose open and shutdown actions again for the next 12 hours. At stage 2, his payoff of stage 1 - 2 is \$0 if he takes the shutdown action at stage 1, or he will lose another \$10 if he is still mining. After a simple probability calculation, it's not hard to find out that the expectation revenue of Figure 3 is higher than Figure 2, showing that a properly applied real option can provide financial advantage for the miner.

In practice, however, the probability and the future price are unknown a priori. Thus, to analyse the tolerance and

revenue, we apply the real option pricing model (as presented in Section II) into the shutdown tolerance analysis. In this model, P^t is the current coin price, the shutdown price $\bar{P}_i^t$ is the strike price of the option, the length of an epoch l can be the life to expiration of the option, and we maintain the traditional options notations r and σ^2 representing risk-less interest rate and variance of the historical coin price, respectively. With our shutdown price model parameters fit into the real option pricing model, we now give a numerical example for a better straightforward illustration.

Example: One mining machine shutdown price is \$6100, the current coin price is also \$6100. One call option has the exercise price as \$6000, the expiration of this option is in 24 hours (one day later), the risk-free interest rate is 5% per annum, and the volatility of the coin price is 20% per annum.

This means that $S_0 = P^t = 6100, K = \bar{P}_i^t = 6000, r = 0.05, \sigma = 0.2$, and $l = 1/365$. Applying Equations 2, 3 and 4, we can get

$$d_1 = \frac{\ln(6100/6000) + \left(0.05 + 0.2^2/2\right) \times (1/365)}{0.2\sqrt{(1/365)}} = 1.597,$$

$$d_2 = \frac{\ln(6100/6000) + \left(0.05 - 0.2^2/2\right) \times (1/365)}{0.2\sqrt{(1/365)}} = 1.587,$$

and

$$S_0 e^{-rT} = 6000 e^{-0.05 \times (1/365)} = 5999.178.$$

Hence, the real option European call is given by

$$Call = 6100 \cdot N(1.59735) - 5999.178 \cdot N(1.58685) = 106.520$$

As demonstrated in the above example, real option theory can nicely describe the shutdown tolerance problem. This elusive right actually gives the miners flexibility, that is, they can learn and adjust their behavior with the market. Therefore, real option advocates that a premium should be paid on the DCF value estimates. The value of the call option, in our example is \$106.520, means that the miner is long for the coin price, or looking forward to the increase of the price so that this machine can keep mining. The machine shutdown price in our example is \$6100, the coin market price is triggering its threshold, and the miner's tolerance bottom line for the this machine is \$6000 (one day after, if the price goes down to \$6000, he would like to switch it off finally), so the value of the right for the miner to tolerate the market price go to \$6000 is \$106.520. Refer to the Equation 1 in Section II, for example, one day after the coin price recovers to \$7000, then the payoff of this option is $max(S_T - K - \epsilon_o, -\epsilon_o) = 7000 - 6000 - 106.520$ = \$893.480, which is a positive revenue for the miner.

Risk-hedging for shutdown tolerance

Furthermore, smarter miners can even better hedge risks, or lower the variance, using the 'percentage shutdown' strategy. More specifically, a miner can choose to shutdown a percentage of shutdown triggered machines immediately to have a higher payoff expectation with less variance. This strategy actually is the 'frequent' style of real option, that is to say, there are multiple embedded real options in the strategy. A miner could divide the same observation time l into four equal periods, if the coin price remain lower than the shutdown price, the miner could shutdown, for example, 25% of his triggered machines each time, which can be considered as learning and adjusting behaviors on a more granular level.

C. Factors Influencing the Shutdown Price.

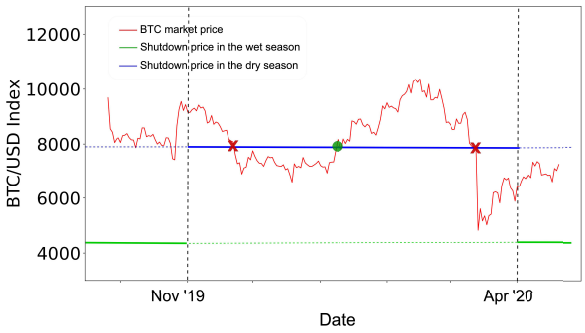

Fig. 4: Antminer T9+ shutdown-open mechanism. The red line represents the BTC market price in USD. The green line represents the shutdown price with low electricity fees in the wet season, while the blue line represents the shutdown price with high electricity fees in the dry season. The red X represents the shutdown point for this mining machine, when BTC price decreases and triggers that point, the machine should be switched off, while the green circle represents the re-open point, when the BTC price hits the point upward, the machine should be switched on.

There are two types of parameters when calculating the shutdown price, i.e., constant and variable parameters. As defined in Equation 6, for a mining machine m_i^t, its mining power h_i^t, the length l of an epoch, and the maximum power consumption $\bar{w}_i$ are constant. The variable parameters, which make the shutdown price dynamic, include the collective mining power H^t, the electricity price E^t, the number of reward coins C, and the coin price P^t. While the coin price P^t may change dramatically within a short time period, the collective mining power H^t, the electricity price E^t, and the number C of coins are relatively stable.

Figure 1 presents the changes of P^t, H^t, and C over time in Bitcoin. The number C of reward coins for mining consists of two parts, namely the block reward and transaction fees. While the transaction fees are fairly stable, the block reward has a dramatic change periodically due to the special event called reward halving [6]. As the Figure 1 shows, a wave of shutdown (i.e., the drop of hashrate) happened immediately on May 11 2020 due to the recent halving event. There are also shutdown

waves because of the falling coin price, for example, in Nov-Dec 2018 when it dropped by almost half of the year-high hashrate, or 12 May 2020 (the 312 event) when the hashrate dropped by 16% overnight that this big fall can lead more than 60% types of BTC mining machines shutdown. A more detailed analysis on different types of mining machines can be found in Table V of Appendix D.

While the electricity price E^t is normally stable over a relatively longer period (e.g. weeks or months), Bitcoin miners are known to use sources of energy that are subjected to *seasonal energy price* variations [36]. For example, the hydroelectric power industry in Sichuan (China[2]) has dry and wet seasons. The electricity price can double when changing the season – wet season (May-October) has low electricity price (0.15-0.20 RMB/ KWh) and the fee can doubled (0.35-0.40 RMB/ KWh) in the dry season (November-April) [13], [16]. This has a significant impact on the shutdown price. Figure 4 taking Antminer T9+ 10.5T[3] as the example illustrates the impact of the seasonal energy price on the shutdown price.

Clustering mining machines. We define the power efficiency as the consumed energy to provide a unit of mining power. The power efficiency significantly varies from one type of mining machine to the other. It also has a great impact on the shutdown price of a type of mining machine – a machine with better power efficiency consumes less energy to provide the same amount of hash power, thus the maintenance cost is cheaper in terms of the electricity fees. To illustrate the efficiency difference among different mining machines, we take all current 101 types of SHA-256 mining machines [30] for a K-means cluster analysis, as shown in the Figure 5, there are 4 main clusters based on mining machine's electricity power consumption, and clusters information is listed in Table I.

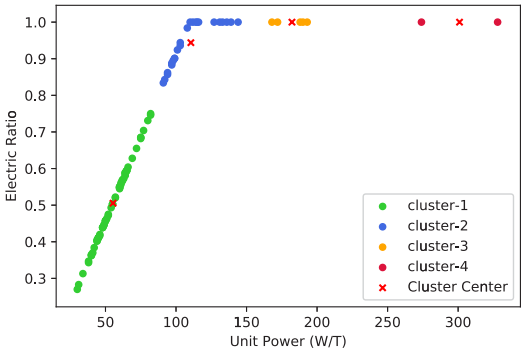

Fig. 5: Different mining machine types k-means clustering. SHA-256D 121 types of mining machines (see full information of the mining machines and their corresponding shutdown prices in Appendix D) are classified based on power efficiency hierarchy into 4 clusters.

[2]China is reported to contribute the most hashrate, mining manufacturer, farms, and pools in the Bitcoin network [17].

[3]Hashrate is a unit measured in hashes per second or H/s: 1EH/s = 1,000 TH/s = 1,000,000 GH/s = 1,000,000,000 MH/s = 1,000,000,000,000 kH/s

We further analyse the relationship between BTC market price and the shutdown price of different clusters of mining machines before and after halving. Figure 6 demonstrates the gap between the coin price and shutdown price of each cluster as well as their shutdown/open status. When the gap is positive, i.e., the BTC market price is higher than the cluster's center shutdown price, the mining machines in this cluster can probably keep mining. But if the gap is negative, means the BTC price is lower than the shutdown price of the cluster center, for example, after halving, cluster-4 can re-open only if the BTC market price increased roughy by $18000, which is around $30000 per Bitcoin.

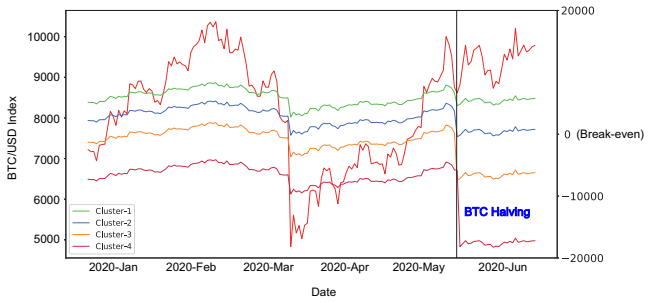

Fig. 6: The gap between the BTC market price and the cluster's shutdown price. The red line represents BTC market price in USD scaled by the left-hand side y-axis. The other four lines represent the gap between the BTC/USD Index and shutdown price (i.e., BTC price - shutdown price) of the center of the four clusters scaled by the right-hand side y-axis.

For simplicity, we consider that the attack happens within one energy season rather than across seasons. But we would like to point out that a transition from wet to dry season can further potentialise this type of attack.

The Bitcoin halving season can be an opportune time for potential attackers. But note that attacks considering shutdown price is a more general idea, no matter if Bitcoin price goes down enough or if a halving happened, as long as there are enough mining machines shutdown in the network, then there is an opportunity for the attack.

While the above discussed factors may change over time, the value of the variables are also different from one cryprocurrency to another. In particular, when a mining machine is compatible with mining in more than one cryptocurrencies, the shutdown price for a machine depends on the cryptocurrency it performs mining on. So if the shutdown price of a mining machine for mining on a cryptocurrency is reached, it may move to mine other cryptocurrencies with compatible mining algorithms.

D. Impact of Shutdown Price

When the shutdown price of some types of mining machines is reached, the miner have the following rational options:

Case 1. Shutdown directly. The miner has no alternative choice except shutdown the machine.

TABLE I: Cluster's Information

Number	Lower Bound	$\bar{P}_i^t$ Before Halving ($)	$\bar{P}_i^t$ After Halving ($)	Upper Bound	$\bar{P}_i^t$ Before Halving ($)	$\bar{P}_i^t$ After Halving ($)
C-1	WhatsM21S 50T	2985.38	5427.97	AntS19 Pro 110T	114597	2629.04
C-2	AntT9+ 10.5T	7038.14	12796.61	InnoT3 50T	3034.32	5516.95
C-3	WhatsM3+ 12T	9461.86	17203.39	EbitE9+ 9T	8211.16	14929.38
C-4	AntV9 4T	16028.07	29141.95	AntS7 4.7T	13432.66	24423.01

Case 2. Mine other coins. When multiple coins share the same mining algorithm, this type of mining machine can transfer to another coin as long as it is still profitable.

Case 3. Rent out mining power. If there exists buyers who are willing to accept these power, the miner can rent or sell them out with a price bigger than the shutdown price. This can be done, for example, via a mining marketplace as NiceHash [27].

Case 4. Behave maliciously. The owner may leverage the mining power to launch attacks for getting a better revenue.

When considering potential 51% attacks, any of the above four cases would make the attacker's job easier as the total honest mining power in the system is reduced. The attacker's profit can be further improved by leveraging *financial derivatives*. Appendix C provides a more detailed discussion.

IV. Related Work

Blockchain platforms such as F2pool [13] and Poolin [30] provide services to indicate the current mining revenue, which can help miners to decide whether or not to shut down a mining machine.

Bonneau [18] identified several bribery attacks to temporarily control a majority of hash power and launch 51% attacks. Alternative methods to bribe miners through higher transaction fees have also been explored [19], [23], [35]. Kwon et al. [21] observed that a miner may gain extra profit by performing honest mining on two blockchains (e.g. BTC and BCH), and proposed a game to model and analyse such behavior. Han et al. [32] described two profit-driven cases where blockchains adapt compatible mining algorithms. One of them is called mining power migration, where mining power from a blockchain with more total mining power is used to attack the blockchain with less mining power in total. The second case is renting cloud mining power to launch a 51% attack. Both cases challenge the honest majority assumption of permissionless blockchains. Yu et al. [37] provided a first study on systems tolerating 51% attacks. They consider miners' reputation as their stake to run a weighted voting scheme, where the reputation is calculated by using a miner's accumulated good work in the system. Eyal and Sirer [12] introduced the selfish mining strategy, where a malicious miner may be able to launch double spending attack with a minority of mining power by temporarily withholding mined blocks. Eyal [10] modeled a game between two mining pools using such block withholding method.

From the financial perspective, Kroll et al. [20] considered a new class of attack which they called Goldfinger attack. The attacker's incentive is outside of the Bitcoin economy and the attacker wishes to see the crash of Bitcoin, or equally, the attacker may hold a significant short positions in Bitcoin. Bonneau [7] revisited the notion of Goldfinger attacks and provided an analysis on the differences between PoW and PoS systems in the face of such extrinsically motivated adversary. Lee and Kim [22] modeled the method to launch a 51% attack on PoS blockchains with short-selling. It shows how an attacker can make a profit despite of the significant depreciation of its underlying cryptocurrency. Han et al. [31] modelled atomic swap as American call option. The shutdown price and derivatives analysed in this paper might be leveraged by an adversary to gain extra profit in the above mentioned works.

V. Discussion

We discuss some of the observations and concerns that have not been covered in the previous sections, including the importance of the electricity price for mining, the difficulty of predicting the change of coin price, and the advantage of stakeholders.

A. Electricity price is a key. From our shutdown price analysis, it becomes clear that the electricity fee is a crucial variable which can decide whether a certain type of mining machine should be switched off or not. Beyond that, electricity is actually the key point to the Bitcoin network security. If the electricity fee becomes cheaper and cheaper for all participants, then theoretically miners will open all the mining machines for mining, therefore increasing the overall hashrate of the network and helping secure the blockchain. Hence, if the electricity fees could be cheap enough, the network could maintain its security even if there are less and less newly minted Bitcoins per block. On the other hand, we should remark that if a miner can get access to much cheaper energy than the other miners, this can help him launch an attack against the blockchain, especially during a halving season.

B. Coin price may not behave as preconceived. Although financial instruments can amplify the profit, they introduce extra risks at the same time. The crucial factor for winning a derivative contract is the price trend of the underlying asset. Theoretically, if the whole ecosystem learned that a cryptocurrency, such as Bitcoin, is not safe anymore, people would tend to give up their investment in Bitcoin. This may lead to a price decrease. However, if the attacker can choose appropriate financial tools such as options in the derivatives market, then

even if the BTC price does not go as preconceived, the attacker can only lose limited contract fees.

C. Insider's advantage. Mining pools' controllers (or even powerful miners) can launch attacks with first-hand information, e.g., hash distribution of each type of mining machine, or where and how to manipulate necessary mining power. In other words, to attack or not is a more informed choice for them. When cryptocurrencies are in situation in which a significant proportion of mining machines shutdown and mining activity itself is less profitable than usual, the security of these blockchains is highly correlated to the super players' personal choices.

VI. Conclusion

In this paper we presented and analysed the concept of shutdown price of mining machines. As an overlooked but important factor for the blockchain security, shutdown price is the point at which operating a mining rig becomes unprofitable. Therefore, miners would switch off the break-even triggered machines. This, in turn, reduces the total network hashrate and makes the system less secure. Besides, we applied real option theory to describe the shutdown decision making process of the miners for better risk-hedging.

The shutdown price can be an indicator for an attacker to seek a good window of time for launching an attack. Meanwhile, it is possible to make a profit by cleverly trading financial derivatives on cryptocurrencies and performing an attack at the same time. The shutdown price can have different impacts under different attacking settings (e.g., selfish mining) and its relationship with the network security deserves further exploration.

References

[1] Baraniuk, C.: Bitcoin's energy consumption 'equals that of Switzerland' - BBC news (Jul 2019), https://www.bbc.com/news/technology-48853230, [Online; accessed 10-May-2020]

[2] Benninga, Simon and Tolkowsky, Efrat: Real options—an introduction and an application to R&D valuation. The Engineering Economist **47**(2), 151–168 (2002)

[3] Binance Blog: Here's What You Need To Know About Binance Options — Binance Blog (2020), https://www.binance.com/en/blog/421499824684900519/Heres-What-You-Need-To-Know-About-Binance-Options, [Online; accessed 15-May-2020]

[4] Bitcoin.org. 51% Attack, Majority Hash Rate Attack. https://bitcoin.org/en/glossary/51-percent-attack (2017), [Online; accessed 11-Jun-2020]

[5] Bitcoin Wiki: Double-spending attacks. https://en.bitcoin.it/wiki/Double-spending (2017), [Online; accessed 11-Jun-2020]

[6] Blockin: Halving Countdown - Blockin Blockchain Explorer (2020), https://www.blockin.com/countdown, [Online; accessed 15-Mar-2020]

[7] Bonneau, Joseph: Hostile blockchain takeovers (short paper). In: International Conference on Financial Cryptography and Data Security. pp. 92–100. Springer (2018)

[8] Damodaran, Aswath: Investment valuation: Tools and techniques for determining the value of any asset, vol. 666. John Wiley & Sons (2012)

[9] Douceur, J.R.: The sybil attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds.) Peer-to-Peer Systems. pp. 251–260. Springer Berlin Heidelberg, Berlin, Heidelberg (2002)

[10] Eyal, I.: The miner's dilemma. In: 2015 IEEE Symposium on Security and Privacy. pp. 89–103. IEEE (2015)

[11] Eyal, I., Sirer, E.G.: Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In: 18th International Conference on Financial Cryptography and Data Security, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers. pp. 436–454 (2014)

[12] Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: International conference on financial cryptography and data security. pp. 436–454. Springer (2014)

[13] F2Pool: F2Pool: Leading Bitcoin, Ethereum & Litecoin Mining Pool (2020), https://www.f2pool.com/, [Online; accessed 10-Jun-2020]

[14] Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol: Analysis and applications. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 281–310. Springer (2015)

[15] Hull, J., et al.: Options, futures and other derivatives/John C. Hull. Upper Saddle River, NJ: Prentice Hall, (2009)

[16] Jamie Redman: 1 Cent per Kilowatt-Hour: China's Sichuan Province Encourages Hydro-Powered Bitcoin Mining — Mining Bitcoin News (2020), https://news.bitcoin.com, [Online; accessed 15-Jun-2020]

[17] Jennifer Wang, Johnson Xu and Wayne Zhao: TI-2019 Mining Industry Annual Report-201912 (2020), https://tokeninsight.com/report/1034?lang=en, [Online; accessed 15-Jun-2020]

[18] Joseph Bonneau: Why Buy When You Can Rent? - Bribery Attacks on Bitcoin-Style Consensus. In: Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers. pp. 19–26 (2016)

[19] Judmayer, A., Stifter, N., Zamyatin, A., Tsabary, I., Eyal, I., Gazi, P., Meiklejohn, S., Weippl, E.: Pay-to-win: Incentive attacks on proof-of-work cryptocurrencies. Tech. rep., Cryptology ePrint Archive, Report 2019/775 (2019)

[20] Kroll, J.A., Davey, I.C., Felten, E.W.: The economics of bitcoin mining, or bitcoin in the presence of adversaries. In: Proceedings of WEIS. vol. 2013, p. 11 (2013)

[21] Kwon, Y., Kim, H., Shin, J., Kim, Y.: Bitcoin vs. bitcoin cash: Coexistence or downfall of bitcoin cash? In: 2019 IEEE Symposium on Security and Privacy (SP). pp. 935–951. IEEE (2019)

[22] Lee, S., Kim, S.: Short selling attack: A self-destructive but profitable 51% attack on pos blockchains. Cryptology ePrint Archive, Report 2020/019 (2020), https://eprint.iacr.org/2020/019

[23] Liao, K., Katz, J.: Incentivizing blockchain forks via whale transactions. In: International Conference on Financial Cryptography and Data Security. pp. 264–279. Springer (2017)

[24] MXC: BTC3L/USDT - MXC - Bitcoin, Litecoin and Ethereum Exchange and Margin, ETF and Futures Trading (2020), https://www.mxc.io/trade/pro\#BTC3L_USDT, [Online; accessed 10-May-2020]

[25] Nakamoto, S., Bitcoin, A.: A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf (2008)

[26] Natoli, C., Yu, J., Gramoli, V., Esteves-Verissimo, P.: Deconstructing blockchains: A comprehensive survey on consensus, membership and structure (2019)

[27] NiceHash: Leading Cryptocurrency Platform for Mining and Trading — NiceHash (2020), https://www.nicehash.com/, [Online; accessed 10-May-2020]

[28] O'Dwyer, K.J., Malone, D.: Bitcoin mining and its energy footprint. In: ISSC/CIICT 2014. pp. 280–285 (2014)

[29] OKEx: The World's Leading One-Stop Crypto Exchange (2020), https://www.okex.com/

[30] Poolin: Poolin.com Pool: Better BTC,BCH,LTC,ZEC,DASH,ETN Cryptocurrency Mining Pool (2020), https://www.poolin.com/, [Online; accessed 10-Jun-2020]

[31] Runchao Han and Haoyu Lin and Jiangshan Yu: On the optionality and fairness of Atomic Swaps. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, October 21-23, 2019. pp. 62–75. ACM (2019)

[32] Runchao Han and Zhimei Sui and Jiangshan Yu and Joseph Liu and Shiping Chen: Fact and Fiction: Challenging the Honest Majority Assumption of Permissionless Blockchains. Cryptology ePrint Archive, Report 2019/752 (2019), https://eprint.iacr.org/2019/752

[33] Wikipedia: Bitcoin gold — Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Bitcoin_Gold (2020), [Online; accessed 23-Sep-2020]

[34] Wikipedia: Ethereum classic — Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Ethereum_Classic (2020), [Online; accessed 23-Sep-2020]

[35] Winzer, F., Herd, B., Faust, S.: Temporary censorship attacks in the presence of rational miners. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 357–366. IEEE (2019)

[36] Wolfie Zhao: China's Rainy Season Is Coming. This Time Bitcoin Miners Aren't Investing - CoinDesk (2020), https://www.coindesk.com/chinas-rainy-season-is-coming-this-time-bitcoin-miners-arent-investing, [Online; accessed 10-Sep-2020]
[37] Yu, J., Kozhaya, D., Decouchant, J., Veríssimo, P.J.E.: Repucoin: Your reputation is your power. IEEE Trans. Computers **68**(8), 1225–1237 (2019)

APPENDIX

A. Notations

Table II presents a summary of notations used in this paper.

B. Financial Derivatives

This section gives an overview of financial derivatives and its pricing which is related to shutdown price analysis and attack's payoff calculation.

1) Financial Derivatives: Financial derivatives are common and popular in traditional financial markets. A *derivative* can be defined as a financial instrument whose value depends on (or derives from) the value of the *underlying asset*. Very often the variables underlying derivatives are the prices of traded assets. A stock option, for example, is a derivative whose value depends on the price of a stock.

Short-selling is one of the most important features of financial instruments. Buyers are referred to as having long positions while sellers are referred to as having short positions. Short selling usually simply referred to as 'shorting' is done with the expectation that the future price of the underlying asset will fall. Short-selling is possible for many (but not all) investment assets. In general, futures contracts, options and ETFs are very common methods to short certain assets in traditional finance markets, and markets can even provide leverage to magnify the profit [15].

In the cryptocurrency world, before 2019, mainstream exchanges such as Coinbase only provided spot trading, i.e., the direct exchange between different coins. However, exchanges are gradually expanding their product lines and including derivatives products similar to the ones in the traditional financial markets. Today, the six financial products that are described in Table III in appendix are already available in crypto exchanges. Investors can already assume short and long positions on cryptocurrencies, and they can even choose coin margined derivatives or fiat (mainly USD) margined derivatives depending on their preferences of monetary unit of measurement.

2) Futures: A *futures contract* is an agreement between two parties to buy or sell an asset at a certain future time for a certain price. It can be contrasted with a *spot contract*, which is an agreement to buy or sell an asset almost immediately. One of the parties to a futures contract assumes a *long position* and agrees to buy the underlying asset on a certain specified future date for a certain specified price. The other party assumes a *short position* and agrees to sell the asset on that date and price. *Contract size* specifies the amount of the asset that has to be delivered under one contract. The payoff of a futures contract can be positive or negative. In general, the payoff from a position on one unit of an asset is

$$\Lambda(S_T - K),$$

where K is the delivery price and S_T is the spot price of the asset at maturity of the contract (as the holder of the contract is obligated to buy an asset worth S_T for K), and the constant $\Lambda \in \{1, -1\}$ has a value of 1 for a long position and of -1 for a short position.

However, the vast majority of futures contracts do not lead to delivery. The reason is that most traders *close out their positions* prior to the delivery period specified in the contract. Closing out a position means entering into the opposite trade to the original one, so that they can realize the profit or loss before the delivery. To open a position, futures contract normally require *margin* as the financial resources to honor the agreement, for the reason that either party may regret the deal and try to back out, and one of the key roles of the exchange is to organize trading so that contract defaults are avoided. This is where margin accounts come in. Note that margin requirements are the same on short futures positions as they are on long futures positions. It is just as easy to take a short futures position as it is to take a long one. The spot market does not have this symmetry.

3) ETF: A traditional *exchange-traded fund (ETF)* is an investment fund tracking an index, such as a stock index or bond index, that traded on stock exchanges. ETFs can be attractive as investments because of their low costs, tax efficiency, and stock-like features. *Leveraged ETFs* are a more aggressive type of ETF that attempt to achieve returns that are more sensitive to market movements than non-leveraged ETFs. Leveraged index ETFs are often marketed as *bull* or *bear* funds based on the directions they choose, for example, a leveraged bull ETF fund might attempt to achieve daily returns that are 2x or 3x more pronounced than the underlying index. In addition, leveraged ETF is a perpetual contract with no settlement day, that is to say, investors are able to buy or sell it at any time with no need of margin.

4) Options: Compared with other financial instruments, an options contract is a more complicated financial derivative. An *options contract* give the contract holder the right to buy or sell an underlying asset on a fixed day in the future. A *call option* gives the holder the right to buy the underlying asset by a certain date for a certain price, while a *put option* corresponds to selling.

The price in the contract is known as the *strike price* or *exercise price*, the date on which the option expires in the contract is known as the *expiration date* or *maturity*. *American options* can be exercised at any time up to the expiration date, while *European options* can be exercised only on the expiration date itself. The *option premium* ϵ_o is the price for this option contract.

An option contract provides the holder with the right to buy or sell a specified quantity of an underlying asset at a fixed price (i.e., strike price / exercise price) at or before the expiration. There has to be a clearly defined underlying asset

TABLE II: Notation and Description

Notation	Description
m_i^t	A mining machine with index i in the t-th epoch.
$\mathcal{M}^t$	The set of mining machines in the t-th epoch, where $\mathcal{M}^t = [m_i^t]_{i=1}^n$.
h_i^t	The mining power of each mining machine m_i^t.
H^t	The collective mining power in the network at the t-th epoch, i.e., $H^t = \sum_{i=1}^n h_i^t$.
$\bar{w}_i$	The power consumption of mining machine m_i
E^t	The average price of electricity (USD/KWh) at the t-th epoch.
C	The average number of coins given to the entire network per epoch, including all new minted coins and transaction fees.
P^t	The average price of the coin (USD per coin) at the t-th epoch.
l	The length (number of hours) of an epoch be l.
R_i^t	The net revenue of miner m_i^t at the t-th epoch.
$\bar{P}_i^t$	The shutdown price of mining machine m_i^t at the t-th epoch.
θ	Shutdown tolerance parameter.
S_0	Current value of the underlying asset
T	The life to expiration of the financial derivatives.
S_T	The value of the underlying asset when closing out the derivatives contract.
K	The strike price.
ϵ_o	The option premium.
r	The risk-less interest rate.
σ^2	The variance of the underlying asset.
$N(x)$	The cumulative probability distribution function for a variable with a standard normal distribution.
Δ	The percentage of coin price decrease.
C_{unit}	The derivatives contract size.
N_c	The number of derivatives contract.
$U_{futures}$	The payoff of futures contract.
U_{ETF}	The payoff of ETF contract.
$U_{options}$	The payoff of options contract.

TABLE III: Cryptocurrency Exchanges Products

Name	Description	Available Exchanges
Spot Trading	The exchange between different cryptocurrencies, using one type of coin as the unit of valuation to buy another coin.	Huobi Global, Coinbase, etc.
Margin Trading	Users can borrow (with multiple leverage options) cryptocurrencies from the exchanges to trade, increasing both benefits and risks.	Huobi Global, Binance, etc.
Futures	Users can choose to buy long or short contracts based on their expectations of how the market will move.	Huobi Global, Binance, etc.
Perpetual Swap	A never-expiring contract that supports choosing to buy long or short contracts to earn, and also has simple operations.	OKEx, Binance, etc.
Options	Users get the right to buy or sell an underlying asset on a fixed day in the future, thus providing the contract holder an opportunity for unlimited profit with limited risk.	OKEx, Bakkt, etc.
Leveraged ETF	A product that tracks the yield rate of the underlying assets with a certain leverage factor.	MXC, etc.

whose value changes overtime in unpredictable ways. The payoffs on this asset have to be contingent on an specified event occurring within a finite period. The contract holder can choose to exercise the option if it is beneficial from doing so, correspondingly, the contract seller is obliged to pay the relevant amount to the contract holder if the option is exercised. If there is no benefit from exercising, the holder can choose not to exercise it with the limited loss of the contract premium itself, then the seller does not need to pay anything in this case.

Figure 7 illustrates the payoffs of four types of option positions: 1. A long position in a call option; 2. A long position in a put option; 3. A short position in a call option; 4. A short position in a put option. To see the payoffs of an options contract, let T be the expiration date, K be the strike price, and S_T be the price asset at maturity, and each options contract worth a premium ϵ_o, which is the cost of buying such an option.

So the payoff of a long position in a European call option is

$$max(S_T - K - \epsilon_o, -\epsilon_o).$$

This reflects the fact that the option will be exercised if $S_T > (K + \epsilon_o)$ and will not be exercised if $S_T \leq (K + \epsilon_o)$.

The payoff of a short position in the European call option is

$$-max(S_T - K - \epsilon_o, -\epsilon_o) = min(K - S_T + \epsilon_o, +\epsilon_o).$$

The payoff of a long position in a European put option is

$$max(K - S_T - \epsilon_o, -\epsilon_o).$$

and the payoff from a short position in a European put option is

$$-max(K - S_T - \epsilon_o, -\epsilon_o) = min(S_T - K + \epsilon_o, +\epsilon_o).$$

For pricing an option, or what is the price of this premium, there are two principles: replication and non-arbitrage. The objective in creating a replicating portfolio is to use a combination of risk-free borrowing/lending and the underlying asset to create the same cash flows as the option being valued: **1. call = borrowing + buying certain amount of the underlying asset; 2. put = short-selling certain underlying asset + lending.** The number of shares bought or sold is called the option delta. Then the principles of arbitrage can apply, and the value of the option has to be equal to the value of the replicating portfolio.

The Black–Scholes model achieved a major breakthrough in the pricing of dividend-protected European options in the limiting distribution settings, and was awarded the Nobel prize for economics in 1997. As the time interval is shortened and goes to zero, the Black-Scholes model applies when the limiting distribution is the normal distribution, and explicitly assumes that the price process is continuous and that there are no jumps in asset prices. The value of a call option can be written as a function of the following variables:

1. S_0 = current value of the underlying asset. As this value increases, the right to buy at a fixed price (call) will become more valuable and the right to sell as a fixed price (put) will become less valuable.

2. K = strike price of the option. The right to buy (sell) at a fixed price becomes more (less) valuable at a lower price;

3. T = life to expiration of the option. Both calls and puts benefit from a longer life;

4. r = risk-less interest rate. As rates increase, the right to buy (sell) at a fixed price in the future becomes more (less) valuable;

5. σ^2 = variance of the underlying asset. As the variance increases, both calls and puts will become more valuable because all options have limited downside and depend upon price volatility for upside.

Therefore, the value of a call option is

$$Call = S_0 N(d_1) - Ke^{-rT} N(d_2)$$

where

$$d_1 = \frac{\ln(S_0/K) + \left(r + \sigma^2/2\right) T}{\sigma\sqrt{T}}$$

$$d_2 = \frac{\ln(S_0/K) + \left(r - \sigma^2/2\right) T}{\sigma\sqrt{T}} = d_1 - \sigma\sqrt{T}$$

The function $N(x)$ is the cumulative probability distribution function for a variable with a standard normal distribution.

The replicating portfolio is embedded in the Black-Scholes model. For example, to replicate this call, you would need to: 1. buy $N(d_1)$ shares of underlying asset, where $N(d_1)$ is called the option delta; 2. borrow $Ke^{-rT} N(d_2)$. The function $N(x)$ is the cumulative probability distribution function for a variable with a standard normal distribution.

C. Attacks Considering Shutdown Price

1) Attacks: Shutdown price is an overlooked yet crucial factor to attacks in PoW-based blockchains. Anyone who controls more than a half of the computational power in the network can re-write the history of the ledger, or we call it as 51% attack. Since it's infeasible for single person to occupy such a large proportion of hashrate, Joseph [18] proposed a novel 51% attack style via bribery that an attacker might purchase a majority of mining power with a premium to temporarily manipulate the network, however, it increases the cost of a potential attack. With the consideration of shutdown price, when coin market price is relatively low and more mining machines triggered their shutdown threshold, attacks taking advantage of this can be considered cheaper and more feasible compared with 'normal' 51% attack and bribery attack.

2) Payoffs of financial derivatives: At the same time, clever attacker can even trade *financial derivatives* when performing an attack for probably better income. Theoretically, a price drop of a cryptocurrency would be expected after a substantial attack on it. In real world, several cryptocurrencies that once had high market cap such as Bitcoin Gold (BTG) [33] and Ethereum Classic (ETC) [34] already witnessed a significant drop of their coin price after crucial security events in the history. The reason is that, when double spending attacks are detected on a cryptocurrency, users may lose their confidence and belief in it. As a consequence, the coin price may drop after the 51% attack, and financial derivatives are the best tools to capture such downwards trend and make a significant profit from it. Therefore, in addition to the double spending income, the financial market can be a further source of profit, which together can help incentivise the attacker in the first place. In this section, we will describe the concepts of financial derivatives and illustrate how they can be used to potentialise an attack.

In this section, we will use the notation S_T for the coin price when closing out the contract, and the parameter Δ $(0 < \Delta < 1)$ to describe the percentage of the coin price decrease, so that we can calculate and compare the incomes of futures contracts, options contracts and leveraged ETFs.

Futures Contract. Futures contract in the cryptocurrency market can be both settled in the coin itself or USD/USDT. On the mainstream cryptocurrency exchange OKEx [29], for example, each contract has a face value of fixed amount of digital token (e.g., BTC/USDT contract has a face value of 0.0001 BTC per contract), and the available range of leverage is 0.01-100x. If the attacker chooses, for example, a BTC contract with 10 times leverage, then he is able to take 1 BTC as the margin to open long/short 10 BTC positions. Considering an attacker short BTC with 4 different futures contracts: Coin Margined Futures 10x, Coin Margined Futures 100x, USDT Margined Futures 10x, USDT Margined Futures 100x, then the income statement is as shown in Table IV.

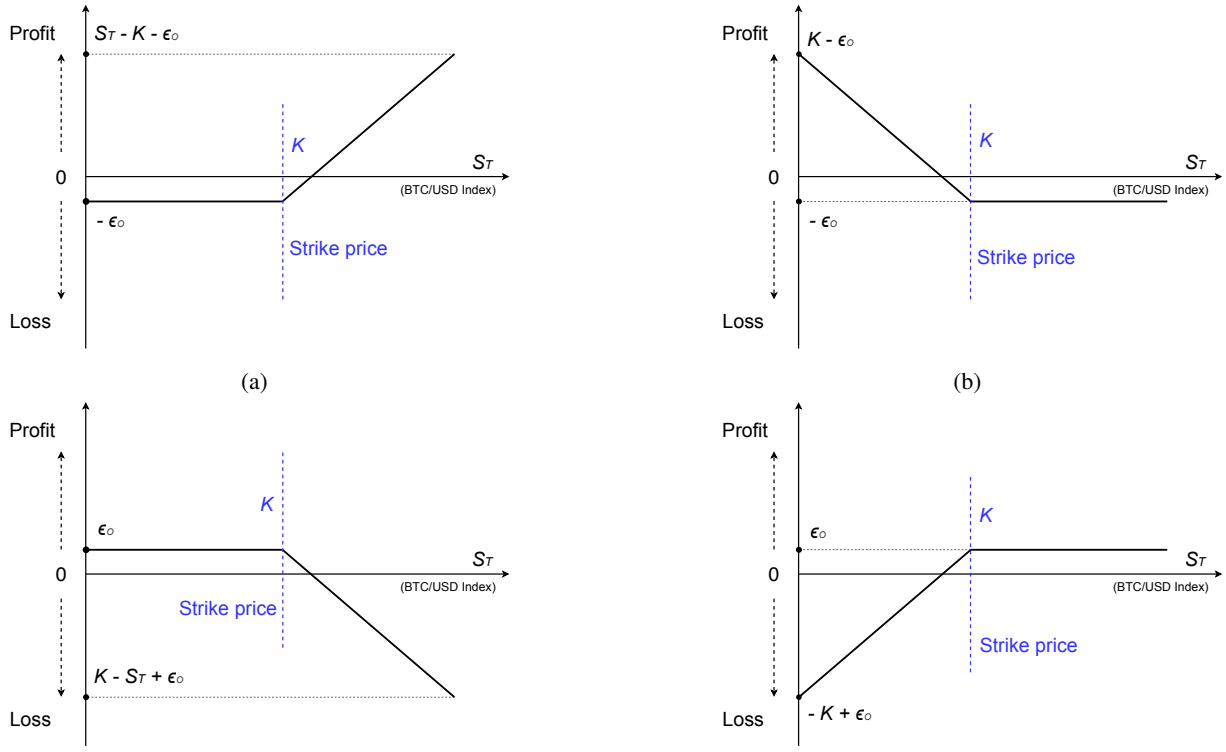

Fig. 7: Payoffs of positions in BTC/USD index European options: (a) long call; (b) short call; (c) long put; (d) short put. X-axis is BTC futures market price in USD denoted as S_T, K is the strike price, ϵ_o is the option premium, Y-axis above 0 represents a profit while below 0 represents a loss.

TABLE IV: Futures Short-selling Income Statement

BTC Price Volatility	Coin Margined Futures 10x	Coin Margined Futures 100x	USDT Margined Futures 10x	USDT Margined Futures 100x
+20%	-200%	-2000%	-200%	-2000%
+10%	-100%	-1000%	-100%	-1000%
-10%	+100%	+1000%	+100%	+1000%
-20%	+200%	+2000%	+200%	+2000%
-30%	+300%	+3000%	+300%	+3000%
-40%	+400%	+4000%	+400%	+4000%
-50%	+500%	+5000%	+500%	+5000%
-60%	+600%	+6000%	+600%	+6000%
-70%	+700%	+7000%	+700%	+7000%
-80%	+800%	+8000%	+800%	+8000%
-90%	+900%	+9000%	+900%	+9000%

To summarize, let N_L be the leverage factor chosen by the attacker, C_{unit} be the contract size, N_c be the number of contract that the attacker bought, so $C_{unit} \cdot N_c$ is the contract principles. If the price decreases, then the payoff of a short position is

$$U_{futures} = C_{unit} \cdot N_c \cdot \Delta \cdot N_L.$$

ETF. MXC [24] currently provides 3x Leveraged ETF with no margin required, the income calculation is quite simple: if the attacker shorts Bitcoin with a leverage factor 3, then when BTC price loses 1%, the net value of the ETF product will rise 3%. Let C_{unit} be the value of the ETF unit, N_c be the number of ETF units that the attacker bought. If the price of Bitcoin decreases, then the payoff of the 3x leveraged ETF is

$$U_{ETF} = 3 \cdot \Delta \cdot C_{unit} \cdot N_c.$$

Options Contract. Among the current options in the cryptocurrency exchange market, Binance options [3] provides the lowest entry barrier for retail users, so we will take Binance options contract here as the example. Binance Options are American-style options, where options can be exercised any time before the expiration date. The underlying asset is BTC/USD Binance futures contract, meaning that it tracks the BTC price from Binance futures market. It is also worth noting

that Binance Options are cash-settled (i.e., USD or USDT), therefore, the physical delivery of the underlying asset is not required.

Upon expiration, an attacker can gain from the fall of BTC/USD Index below the strike price, the lower the price is, the more the attacker can gain. Upon expiration, if the market goes against prediction, the loss is limited to the options premium only. The attacker can decide how many contracts to buy as a leverage in order to amplify the income.

To calculate the payoff of the options contract, let T be the expiration date, K be the Bitcoin strike price, and S_T be the Bitcoin price at maturity after the attack, ϵ_o be the premium of each options contract, N_c be the number of contract that the attacker bought, so the payoff to the attacker in the put option is

$$U_{options} = N_c \cdot max(K - S_T - \epsilon_o, -\epsilon_o).$$

D. Shutdown Price Hierarchy Before and After Halving

Table V shows the shutdown price before and after halving of mainstream BTC mining machines. The data was fetched from Poolin Website [30] on 10th June 2020. The Bitcoin mining information on that day is: BTC/USD Index 9500, network hashate 114.44 EH/s, current difficulty 13.73 T, next difficulty 14.90 T (+8.50%), next difficulty adjustment in 5 days, block reward 6.25 BTC, and electricity fees 0.035 USD/KWh. Symbol ON represents current BTC price is higher than the mining machine shutdown price, the machine status is on. Symbol OFF represents current BTC price is lower than the mining machine shutdown price, the machine status is shutdown.

TABLE V: Mainstream BTC Mining Machine Shutdown Price [30]

Mining Machine	Hashrae (TH/s)	Power (W)	Unit Power (W/T)	Rev.24H ($)	Energy Cost ($)	Electric Ratio	$\bar{P}_i^t$ Before Halving	Profit 24H Before Halving ($)	Shutdown Status	$\bar{P}_i^t$ After Halving	Profit 24H After Halving ($)	Shutdown Status
Antminer V9	4.00	1310	328	0.37	1.10	1.000	16028.07	-0.42	OFF	29141.95	-0.73	OFF
Antminer S7	4.70	1290	274	0.43	1.08	1.000	13432.66	-0.28	OFF	24423.01	-0.65	OFF
Whatsminer M3+	12.00	2320	193	1.10	1.95	1.000	9461.86	0.09	ON	17203.39	-0.85	OFF
Avalon A741	7.30	1390	190	0.67	1.17	1.000	9318.84	0.07	ON	16943.35	-0.50	OFF
Whatsminer M3	11.50	2160	188	1.06	1.81	1.000	9192.34	0.15	ON	16713.34	-0.76	OFF
Avalon A721	6.00	1030	172	0.55	0.87	1.000	8401.48	0.15	ON	15275.42	-0.31	OFF
Ebit Miner E9+	9.00	1510	168	0.83	1.27	1.000	8211.16	0.27	ON	14929.38	-0.44	OFF
Antminer T9+	10.50	1510	144	0.97	1.27	1.000	6900.14	0.52	ON	12906.61	-0.30	OFF
Ebit Miner E9i	13.50	1870	139	1.24	1.57	1.000	6779.19	0.72	ON	12325.80	-0.33	OFF
Ebit Miner E9.3	16.00	2170	136	1.47	1.82	1.000	6637.58	0.90	ON	12068.33	-0.35	OFF
Ebit Miner E10	18.00	2400	133	1.65	2.02	1.000	6525.43	1.03	ON	11864.41	-0.36	OFF
Ebit Miner E9.2	12.00	1570	131	1.10	1.32	1.000	6403.07	0.72	ON	11641.95	-0.22	OFF
Snow Panther A1	49.00	6210	127	4.51	5.22	1.000	6202.48	3.12	ON	11277.24	-0.71	OFF
Avalon A851	14.50	1680	116	1.33	1.41	1.000	5670.37	1.05	ON	10309.76	-0.08	OFF
Avalon A911B	17.00	1950	115	1.56	1.64	1.000	5613.78	1.25	ON	10206.88	-0.07	OFF
Avalon A821	11.00	1250	114	1.01	1.05	1.000	5561.44	0.82	ON	10111.71	-0.04	OFF
Avalon A841	13.00	1450	112	1.20	1.22	1.000	5458.77	1.00	ON	9925.03	-0.02	OFF
Antminer S9i/13.5T	13.50	1490	110	1.24	1.25	1.000	5401.60	1.04	ON	9821.09	-0.01	OFF
Antminer S9i/13T	13.00	1400	108	1.20	1.18	0.984	5270.53	1.04	ON	9582.79	0.02	ON
Antminer S9	13.50	1395	103	1.24	1.17	0.944	5057.21	1.12	ON	9194.92	0.07	ON
Avalon A921	20.00	2050	103	1.84	1.72	0.936	5016.42	1.68	ON	9120.76	0.12	ON
Antminer S9 Hydro	18.00	1820	101	1.65	1.53	0.924	4948.45	1.52	ON	8997.18	0.13	ON
Antminer S9j	14.50	1430	99	1.33	1.20	0.901	4826.56	1.26	ON	8775.57	0.13	ON
Avalon A920	18.00	1750	97	1.65	1.47	0.888	4758.12	1.58	ON	8651.13	0.18	ON
Snow Panther B1	16.00	1510	94	1.47	1.27	0.862	4618.78	1.45	ON	8397.78	0.20	ON
Inno T1	16.00	1500	94	1.47	1.26	0.857	4588.19	1.46	ON	8342.16	0.21	ON
Avalon A911	19.50	1800	92	1.79	1.51	0.843	4517.60	1.80	ON	8213.82	0.28	ON
Inno T2	17.20	1570	91	1.58	1.32	0.834	4467.26	1.60	ON	8122.29	0.26	ON
XINSHILI Q3	30.00	2450	82	2.76	2.06	0.746	3996.82	3.05	ON	7266.95	0.70	ON
Antminer S11	20.50	1530	75	1.88	1.29	0.682	3652.64	2.19	ON	6641.17	0.60	ON
Antminer T15	23.00	1650	72	2.11	1.39	0.655	3510.96	2.51	ON	6383.57	0.73	ON
Inno T2T/32T	32.00	2200	69	2.94	1.85	0.628	3364.67	3.59	ON	6117.58	1.09	ON
Whatsminer M10	33.00	2180	66	3.03	1.83	0.604	3233.05	3.78	ON	5878.27	1.20	ON
Whatsminer M10S	55.00	3575	65	5.06	3.00	0.594	3181.15	6.36	ON	5783.90	2.05	ON
HummerMiner H7pro	53.00	3445	65	4.87	2.89	0.594	3181.15	6.12	ON	5783.90	1.98	ON
Hummer Miner H7pro	48.00	3120	65	4.41	2.62	0.594	3181.15	5.54	ON	5783.90	1.79	ON
Avalon A1047	37.00	2405	65	3.40	2.02	0.594	3181.15	4.27	ON	5783.90	1.38	ON
Avalon A1046	36.00	2320	64	3.31	1.95	0.589	3153.95	4.17	ON	5734.46	1.36	ON
CHEETAH MINER F5M	52.00	3350	64	4.78	2.81	0.589	3152.91	6.03	ON	5732.56	1.97	ON
Avalon A1045	35.00	2250	64	3.22	1.89	0.587	3146.19	4.07	ON	5720.34	1.33	ON
Avalon A1066	50.00	3195	64	4.60	2.68	0.584	3127.31	5.83	ON	5686.02	1.91	ON
Ebit Miner E12	44.00	2800	64	4.05	2.35	0.581	3114.41	5.14	ON	5662.56	1.69	ON
CHEETAH MINER F5	55.00	3450	63	5.06	2.90	0.573	3069.91	6.46	ON	5581.66	2.16	ON
Whatsminer M21S/54T	54.00	3360	62	4.96	2.82	0.569	3045.20	6.36	ON	5536.72	2.14	ON
Whatsminer M21S/56T	56.00	3480	62	5.15	2.92	0.568	3041.31	6.61	ON	5529.66	2.23	ON
Inno T3/50T	50.00	3100	62	4.60	2.60	0.566	3034.32	5.91	ON	5516.95	1.99	ON
Whatsminer M21	28.00	1720	61	2.57	1.44	0.561	3006.36	3.31	ON	5466.10	1.13	ON
Antminer S15	28.00	1690	60	2.57	1.42	0.551	2953.92	3.33	ON	5370.76	1.15	ON
Avalon 1066 Pro	55.00	3300	60	5.06	2.77	0.548	2936.44	6.59	ON	5338.98	2.28	ON
Whatsminer M21S/52T	52.00	3120	60	4.78	2.62	0.548	2936.44	6.22	ON	5338.98	2.16	ON
Avalon A1146	56.00	3340	60	5.15	2.81	0.545	2918.96	6.72	ON	5307.20	2.34	ON
Antminer T17/42T	42.00	2400	57	3.86	2.02	0.522	2796.61	5.12	ON	5084.75	1.85	ON
Inno T3/39T	39.00	2220	57	3.59	1.86	0.520	2785.85	4.78	ON	5065.19	1.72	ON
Antminer T17e/53T	53.00	2915	55	4.87	2.45	0.503	2691.74	6.56	ON	4894.07	2.42	ON
Whatsminer M21S+/62T	62.00	3348	54	5.70	2.81	0.493	2642.79	7.74	ON	4805.08	2.89	ON
Avalon A1146 Pro	63.00	3276	52	5.79	2.75	0.475	2544.92	7.96	ON	4627.12	3.04	ON
Taurus miner C12	62.00	3200	52	5.70	2.69	0.472	2525.97	7.86	ON	4592.67	3.01	ON
Inno T3+ Pro/67T	67.00	3400	51	6.16	2.86	0.464	2483.56	8.54	ON	4515.56	3.30	ON
Whatsminer M20S/65T	65.00	3260	50	5.98	2.74	0.458	2454.56	8.32	ON	4462.84	3.24	ON
Hummer Miner H9	67.00	3350	50	6.16	2.81	0.457	2447.03	8.59	ON	4449.15	3.35	ON
Antminer T17+/64T	64.00	3200	50	5.88	2.69	0.457	2447.03	8.19	ON	4449.15	3.20	ON
Ebit Miner E12+	50.00	2500	50	4.60	2.10	0.457	2447.03	6.41	ON	4449.15	2.50	ON
Avalon A1166	68.00	3325	49	6.25	2.79	0.447	2393.06	8.77	ON	4351.01	3.46	ON
Inno T3/43T	43.00	2100	49	3.95	1.76	0.446	2390.12	5.55	ON	4345.68	2.19	ON
Whatsminer M20S/68T	68.00	3265	48	6.25	2.74	0.439	2349.88	8.82	ON	4272.50	3.51	ON
Whatsminer M20S/70T	70.00	3360	48	6.44	2.82	0.439	2349.15	9.09	ON	4271.19	3.61	ON
Whatsminer M20S/62T	62.00	2976	48	5.70	2.50	0.439	2349.15	8.05	ON	4271.19	3.20	ON
Whatsminer M20	45.00	2160	48	4.14	1.81	0.439	2349.15	5.85	ON	4271.19	2.32	ON
Whatsminer M31S	72.00	3312	46	6.62	2.78	0.420	2251.27	9.47	ON	4093.22	3.84	ON
StrongU U8	46.00	2100	46	4.23	1.76	0.417	2234.25	6.07	ON	4062.27	2.47	ON
Antminer S17e/64T	64.00	2880	45	5.88	2.42	0.411	2202.33	8.46	ON	4004.24	3.47	ON
Antminer S17e/60T	60.00	2700	45	5.52	2.27	0.411	2202.33	7.94	ON	4004.24	3.25	ON
Antminer S17/53T	53.00	2385	45	4.87	2.00	0.411	2202.33	7.01	ON	4004.24	2.87	ON
Ebit Miner E11++	44.00	1980	45	4.05	1.66	0.411	2202.33	5.83	ON	4004.24	2.38	ON
Antminer S17/56T	56.00	2480	44	5.15	2.08	0.405	2167.37	7.45	ON	3940.68	3.07	ON
Whatsminer M20S+/78T	78.00	3432	44	7.17	2.88	0.402	2153.39	10.38	ON	3915.25	4.29	ON
Inno T4+	75.00	3300	44	6.90	2.77	0.402	2153.39	10.00	ON	3915.25	4.12	ON
Whatsminer M31S+	78.00	3276	42	7.17	2.75	0.384	2055.51	10.51	ON	3737.29	4.42	ON
Antminer S17 Pro/56T	56.00	2268	41	5.15	1.91	0.370	1982.10	7.62	ON	3603.81	3.24	ON
Hippo Miner H1	60.00	2400	40	5.52	2.02	0.365	1957.63	8.19	ON	3559.32	3.50	ON
Antminer S17+/73T	73.00	2900	40	6.71	2.44	0.363	1944.22	9.97	ON	3534.94	4.28	ON
Antminer S17 Pro/53T	53.00	2100	40	4.87	1.76	0.362	1939.16	7.25	ON	3525.74	3.11	ON
Whatsminer M30S	88.00	3340	38	8.09	2.81	0.347	1857.52	12.16	ON	3377.31	5.29	ON
Antminer T19	84.00	3150	38	7.72	2.65	0.343	1835.27	11.63	ON	3336.86	5.08	ON
Antminer S19	95.00	3250	34	8.73	2.73	0.313	1674.29	13.42	ON	3044.16	6.00	ON
Whatsminer M30S++	112.00	3472	31	10.30	2.92	0.283	1517.16	16.14	ON	2758.47	7.38	ON
Antminer S19 Pro	110.00	3250	30	10.11	2.73	0.270	1445.97	15.97	ON	2629.04	7.38	ON