The cost of attack on the Decred network can be broken into two components; the work component, W and the stake component T. The attack cost, A, is the sum of the two components.

$$A = W + T \tag{1}$$

These two components are not independent. They are related through $\sigma(y)$, which is the fraction of total network hashrate an attacker would need to control in order to perform an attack, given that they control fraction y of the stakepool tickets. The relation was expressed in [1] as,

$$x(y) = \left(\left(\frac{1}{y} - 1\right) \cdot p\right)^N \tag{2}$$

which is defined as the ratio of the attacker's hashpower to honest hashpower. For calculating network security, the costs can be further minimized by assuming that the attacker's hashpower is already mining honestly on the mainchain before being apruptly redirected to the attacker's chain. Then

$$\sigma(y) = \frac{x(y)}{x(y) + 1} \tag{3}$$

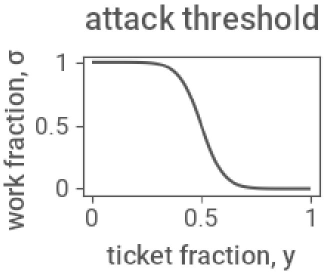

Figure 1: The threshold of hashpower needed to initiate an attack.

σ is the fraction of total network hashrate an attacker would need to redirect if they control fraction y of the tickets in the stake pool, participation ratio p of all tickets' holders are currently online, and N is the number of POS validators per block. Participation ratio p has historically been very near 1. N is a network parameter currently set at 5.

Note that $W \propto \sigma(y)$ and $T \propto y$. The cost of attack is calculated by taking the minimum of $A(y)$ on the interval $[0, 1]$.

1 Work term

The work term, W, is the cost associated with POW mining. The correct form of the work term is complicated by the availability of rental equipment, and as such depends on market rental price and rental availability. The general form is

$$W = \underbrace{R}_{\text{rental}} + \underbrace{D + P}_{\text{retail}} \tag{4}$$

where R is the total costs associated with rental equipment, D is the total cost of purchasing retail devices and associated equipment, and P is the total cost of power over the duration of attack. Rental costs can be calculated given a rental price, r_e, (units price/hash) and a "rentability", a, which represents the total rental hashing power available in units of hashrate. For an attack duration t_a, the rental costs are

$$R = ar_e t_a. \tag{5}$$

If there is not enough rentability to supply the attacker's hashpower threshold, retail equipment supplies the remainder. To calculate retail costs, key equipment parameters can be estimated from the device performance and retail market price of state-of-the-art hardware. Devices will have a hashrate h_d, a power draw ω_d, and a retail cost p_d, which should include some amount of overhead associated with support equipment, i.e. power supplies, cabling, etc. Device parameters are ultimately expressed in terms of the power efficiency $\eta = h_d/\omega_d$, and relative cost $\rho = p_d/h_d$. The full retail costs are given by summing the equipment term

$$D = (H_a - a) \cdot \rho \tag{6}$$

with the power term

$$P = \frac{(H_a - a)}{\eta} \cdot c \cdot t_a \tag{7}$$

where H_a is the required attacker hashrate and c is the electricity rate (cost/energy).

The work fraction, or the fraction of network hashrate the attacker would need to redirect, is related to the total network hashrate, H_{net} through equation 1 as

$$H_a = \sigma(y)H_{net}. \tag{8}$$

For further parametrization, it's useful to note the relationship between network hashrate, fiat exchange rate X, miner profitability α, and various network and device parameters (Appendix A).

$$H_{net} = \frac{\beta X}{\alpha\rho + 0.24c/\eta} \tag{9}$$

where β is the total POW rewards (DCR) payed out daily. The benefit of parametrizing in terms of miner profitability is that the value is self-regulating and tends towards zero. β is dependent on various network parameters as

$$\beta = \frac{86400 R_{pow}}{t_b} \tag{10}$$

with R_{pow} the POW block reward, and t_b is the network's target block time. The full block reward, R_{tot}, for Decred is dependent on block height, h.

$$R_{tot}(h) = 31.19582664(100/101)^{floor(h/6144)} \tag{11}$$

At the time of writing, the POW miner is rewarded with 60% of the total block reward, though it will be left as a parameter, s, here; $R_{pow} = sR_{tot}$.

The fully parametrized work term is then

$$W = ar_e t_a + \Big(H_a - a\Big)\Big(\rho + \frac{ct_a}{\eta}\Big) \tag{12}$$

with

$$a \leq H_a = \frac{86400 s\sigma(y) R_{tot}(h) X}{t_b(\alpha\rho + 0.24c/\eta)} \tag{13}$$

Equation 13 assumes units of seconds for block time and fiat/kWh for electricity rate.

2 Stake term

The ticket fraction, y, is the ratio of attacker controlled tickets to all tickets in the stake pool. For an average fiat-converted ticket price, p_t, and a ticket pool size of Z tickets, the stake term is expressed as

$$T = yZp_t \tag{14}$$

The fiat-converted ticket price has shown strong dependence on the exchange rate. Stated otherwise, the stake difficulty has remained relatively constant through the exchange market chaos of 2018.

On the other hand, the ticket price would be expected to have some dependence on the attacker stake ratio, y, because the attacker acquiring a significant portion of the stake pool would undoubtedly cause the ticket price to rise, as the pricing algorithm adjusts for increased demand. That relationship is not explored further here.

3 Application

The attack cost could be used to explore the effects of changing network parameters. Typically this proceeds by starting starting with pararmeter values reflecting current network and market conditions. Parameter space can be explored around this starting point to examine how market and network changes might affect network security.

References

[1] Iddo Bentov et. al. Proof of activity: Extending bitcoin's proof of work via proof of stake. 2014.

Appendices

A Network hashrate and POW profitability

Miner net daily earnings can be written as

$$E_{net} = \alpha p_d = \underbrace{E_g}_{\text{gross profit}} - \underbrace{\frac{24\omega_d c}{1000}}_{\text{power costs}} \tag{15}$$

which defines a profitability, α. The profitability can be thought of as the fraction of device cost retrieved in a day of mining. Profitability self-regulates in that if profitability gets too high, entrepeneurial miners will buy more hashpower and profitability will drop. If profitability drops below zero, it becomes cheaper to buy DCR outright, so miners will turn off their equipment and it will tend towards zero.

The total amount of fiat payed out to miners in a given day can be written in terms of total POW rewards and the fiat exchange rate.

$$Q = \beta X \tag{16}$$

The total number of devices on the network, N_d, can be expressed in two different ways.

$$N_d = \frac{Q}{E_g} = \frac{H_{net}}{h_d} \tag{17}$$

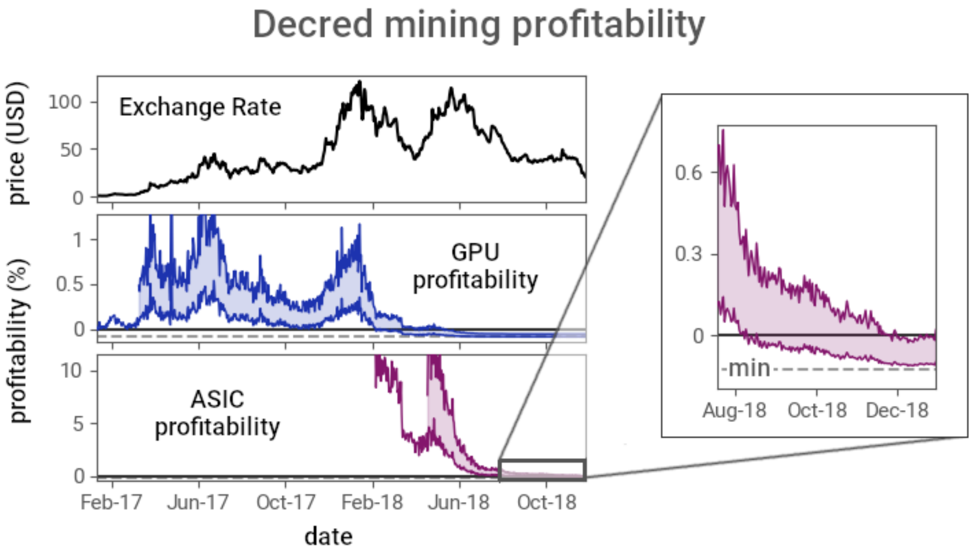

Figure 2: Mining profitability shows immediate response to price spikes, followed by decay towards zero when the price is stable.

Combining this relation with equation 15, and substituting alternative device parameters ρ and η, yields an expression for network hashrate.

$$H_{net} = \frac{\beta X}{\alpha\rho + 0.24c/\eta} \tag{18}$$

in terms of the somewhat predictable profitability term.

symbol	unit	description
A	fiat	Cost of attack. Minimum cost to launch a successful attack on the Decred network.
a	hashes/time	Rentability. Amount of hashing power available on the rental market
α	–	POW profitability. Daily earnings as a fraction of device cost.
β	DCR	POW payout. Total decred paid to POW miners per day.
c	fiat/energy	Electricity rate. Common units of \$/kWh.
D	fiat	Retail equipment cost.
E_g	fiat	Model device gross daily earnings, before power costs.
E_{net}	fiat	Model device net daily earnings.
η	hashrate/power	POW power efficiency. $\eta = h_d/\omega_d$
H_a	hash/time	Hashpower required to be under attacker control.
H_{net}	hash/time	Total network hashpower.
h_d	hash/time	Model device hashrate.
N	–	POS validators per block.
P	fiat	Power costs of attack.
p	–	Participation level. Fraction of tickets which belong to an online stakeholder.
p_d	fiat	Model device price.
p_t	fiat	Ticket price.
ρ	fiat/hashrate	Relative device cost. $\rho = p_d/h_d$
Q	fiat	Total POW payout per day, in fiat.
R	fiat	Rental costs of attack.
R_{pow}	DCR	POW block reward.
R_{tot}	DCR	Total block reward.
r_e	fiat/hash	Rental rate.
s	–	POW reward share. Fraction of R_{tot}. given as a POW reward.
σ	–	Hashportion. The minimum attacker hashpower, as a fraction of total network hashpower.
T	fiat	Stake term. Total cost of attack spent on tickets.
t_a	time	Attack duration. Time required to carry out attack.
t_b	time	Block time. The network block time target.
W	fiat	Work term. Total equipment-related costs of attack.
ω_d	energy/time	Model device power draw.
X	fiat/DCR	Exchange rate.
x	–	Hashrate multiplier. From [1].
y	–	Attacker controlled fraction of the total stake pool.
Z	tickets	Ticket pool size. A network parameter.