Parametrized cost of attack as a measure of Decred network security

Brian Stafford

January 10, 2019

1 Introduction

Due its hybrid concensus protocol, the Decred network presents unique challenges to measuring the network's resiliency to attack. In addition to new proof-of-stake related vulnerabilities, the well known $> 50\%$ hashpower threshold is not constant for Decred. The hashpower threshold also depends on the fraction of stake pool tickets the attacker controls [1]. For an attacker who controls very few tickets, the hashpower threshold is very nearly 100%, but becomes lower with increasing stake.

Proposed here is a measure of network security tentatively named the *parametrized cost of attack* (PCOA), defined roughly as the fiat expenditure required to perform an attack.

The PCOA can be broken into two components; the work component, W and the stake component S. The cost of attack, A, is the sum of the components.

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

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 they control fraction y of the stakepool tickets. If N ticket holders are chosen per block, the probability $P(y)$ that the attacker holds a majority of selected tickets is given by

$$P(y) = \sum_{k=0}^{k<N/2} \binom{N}{k} y^{N-k} \Big((1-y)\cdot p\Big)^k \tag{2}$$

where $\binom{N}{k}$ is a binomial coefficient. N is set to 5 for Decred, but is left as a paremeter here. The participation ratio, p, is the fraction of stakeholders online and ready to vote, and has historically been very nearly 1.

The attacker would hold the majority of tickets on every $1/P(y)$ blocks. Conversely, the honest nodes would be able to achieve consensus on every $1/(1-P(y))$. The attacker would need

$$x(y) = \frac{1/P(y)}{1/(1-P(y))} = \frac{1}{P(y)} - 1 \tag{3}$$

times the honest hashpower in order to outpace the honest chain. This relation gives the first insight into the work term. If the network hashrate, H_{net}, is known, one could, in principle, calculate how much hashing power an attacker would need to control, and see how much it would cost to purchase. But $x(y) \cdot H_{net}$ fails to minimize the costs because of an implicit assumption that the attacker's hashpower is not already a part of the honest network hashpower. Instead, assume that the attacker's hashpower is already mining honestly on the mainchain before being apruptly redirected to the attacker's chain. Then

$$\sigma(y) = \frac{x(y)}{x(y)+1} \tag{4}$$

is the fraction of total network hashrate an attacker would need to redirect.

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

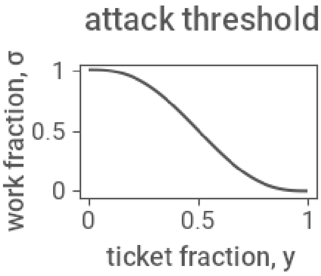

Figure 1: The threshold of hashpower needed to initiate an attack.

2 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

$$W = \underbrace{R}_{\text{rental}} + \underbrace{D + P}_{\text{retail}} \tag{5}$$

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. P is typically small. 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

$$R = ar_e t_a. \tag{6}$$

If there is not enough rentability to meet 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

$$D = (H_a - a) \cdot \rho \tag{7}$$

with the power term

$$P = \frac{(H_a - a)}{\eta} \cdot c \cdot t_a \tag{8}$$

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 3 as

$$H_a = \sigma(y) H_{net}. \tag{9}$$

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

$$H_{net} = \frac{\beta X}{\alpha_w \rho + 0.24c/\eta} \tag{10}$$

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

$$\beta = \frac{86400 R_{pow}}{t_b} \tag{11}$$

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.

$$R_{tot}(h) = 31.19582664(100/101)^{floor(h/6144)} \tag{12}$$

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_w, here; $R_{pow} = s_w R_{tot}$.

The fully parametrized work term is then

$$W = ar_e t_a + \Big(H_a - a\Big)\Big(\rho + \frac{ct_a}{\eta}\Big) \tag{13}$$

with

$$a \leq H_a = \frac{86400 s_w \sigma(y) R_{tot}(h) X}{t_b(\alpha_w \rho + 0.24c/\eta)} \tag{14}$$

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

3 Stake term

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

$$S = yZXp_t \tag{15}$$

Historically, the stake difficulty has shown relative stability, even through chaotic market changes, so variations in the ticket term have mostly followed the fiat exchange rate.

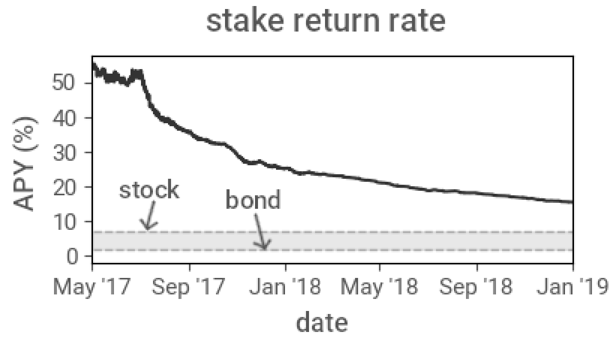

Figure 2: As Decred staking gains acceptance as an investment product, the returns will tend towards those of other common investment products.

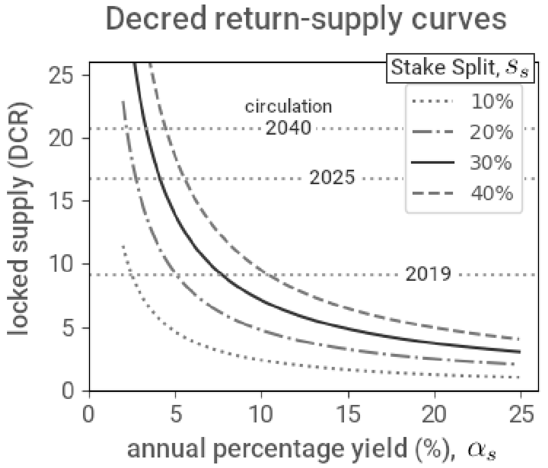

Figure 3: There is a lower limit to the steady state APY where the total stake is equal to the total supply. The position of the limit can be modified by increasing or decreasing the fraction of the block reward given to ticket holders.

In a similar fashion as the work term, the stake term can be further parametrized by noting the relationship between ticket price, block reward, and stake annual percentage yield (APY), α_s,

$$\alpha_s = \left(\frac{p_t + (R_{pos}/N)}{p_t}\right)^{365/28} - 1 \tag{16}$$

with $R_{pos} = s_s R_{tot}$ (s_s is currently set at 0.3). Here again, the return rate is chosen for parametrization due to its tendency towards some natural value. In this case, though, the asymptotoic value is not zero. Instead, as Decred staking gains acceptance as an institutional investment product, the return rate should approach the rates of other common investments. The typical APY of institutional investment products ranges from around 2% for bonds to about 7% for stocks. Because of the limited supply of Decred, there is a lower limit on the steady-state APY possible given by

$$C(t) = p_t Z \rightarrow \alpha_{min} = \left[\frac{Z R_{pos}}{C(t) N} + 1\right]^{365/28} - 1 \tag{17}$$

where $C(t)$ is the total Decred in circulation. This provides a natural lower limit to the range of α_s.

The fully parametrized stake term can then be written.

$$S = \frac{yZXs_sR_{tot}}{N[(\alpha_s + 1)^{28/365} - 1]} \tag{18}$$

4 Application

To make use of the PCOA, typically a starting position in parameter space is chosen, and parameters are varied one or two at a time around that position, treating all other as either constant, or changing in some known way with the chosen variables.

What the ideal block reward split for the current network conditions.

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

$$E_{net} = \alpha_w p_d = \underbrace{E_g}_{\text{gross profit}} - \underbrace{\frac{24\omega_d c}{1000}}_{\text{power costs}} \tag{19}$$

which defines a profitability, α_w. 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 back towards zero.

The fiat value of block rewards payed out to miners in a given day can be written in terms of total POW portion of the block reward, β and the fiat exchange rate.

$$Q = \beta X \tag{20}$$

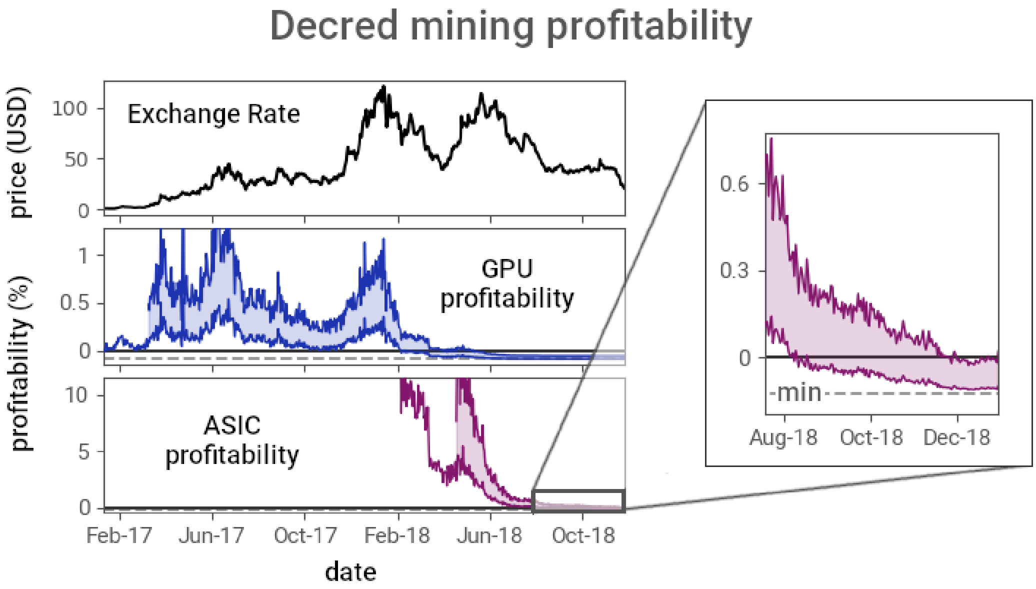

Figure 4: Mining profitability shows immediate response to price spikes, followed by decay towards zero when the price is stable.

Using the model device statistics, the total number of devices on the network, N_d, can be expressed in two different ways.

$$N_d = \frac{Q}{E_g} = \frac{H_{net}}{h_d} \tag{21}$$

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

$$H_{net} = \frac{\beta X}{\alpha_w \rho + 0.24c/\eta} \tag{22}$$

in terms of the somewhat predictable profitability term.

	GPU		ASIC	
	low	high	low	high
η (hashrate /watt)	4.1×10^6	1.8×10^7	3.9×10^8	2.3×10^9
ρ (\$/hashrate)	3.5×10^{-7}	1.3×10^{-7}	2.5×10^{-9}	8.1×10^{-10}

Table 1: Power efficiency, η, and relative cost, ρ, of the model devices used for the ranges in figure 3.

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_w	–	POW profitability. Daily earnings as a fraction of device cost.
α_s	–	Stake return. Annual percentage yield.
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.

symbol	**unit**	**description**
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	fiat	Stake term. Total cost of attack spent on tickets.
s_s	–	POS rewaard share Fraction of R_{tot}. given as a stake reward.
s_w	–	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_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.