Parametrized cost of attack as a measure of Decred network security

Brian Stafford

January 18, 2019

1 Introduction

Due its hybrid concensus protocol, the Decred blockchain presents unique challenges to the measurement of attack resiliency. 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. For an attacker who controls very few tickets, the hashpower threshold is very nearly 100%, but becomes lower with increasing stake (figure 1).

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

Attempts are made below to minimize the PCA, but there are certainly other ways that are not considered here. For example, access to sub-retail equipment, as in the case of a malicious chipmaker, is not considered. Denial-of-service attack components are also not considered, although they certainly deserve attention.

2 Ticket fraction and work fraction

The PCA 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 parameter here. The participation ratio, p, is the fraction of stakeholders online and ready to vote, and has historically been very nearly 1. While participation will be taken to be 1 for the

remainder of this work, it is important to note that p could potentially be a target for a denial-of-service attack component.

The attacker would hold the majority of tickets derived from every $1/P(y)$ valid nonces they are able to generate. Conversely, the honest nodes would be able to achieve consensus on every $1/(1-P(y))$ blocks proposed to the honest network. The attacker would need a factor of

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

times the honest hashpower in order to outpace the honest chain. Using $x(y)$ as a hashrate multiplier to calculate the attacker's required hashpower carries an implicit assumption that the attacker's hashpower is not already part of the existing honest hashpower before the attack. If this assumption is dropped, the threshold can be minimized further. Stated otherwise, assume that the attacker's hashpower is already mining honestly on the main chain before being apruptly redirected to the attacker's chain. Then

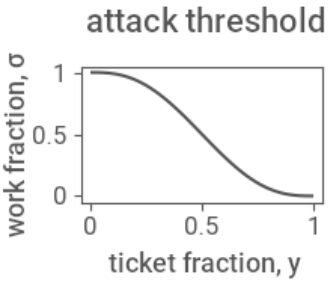

Figure 1: The threshold of hashpower needed to initiate an attack.

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

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

If the network hashrate, H_{net}, is known, then $x(y)$ can be used to calculate how much hashpower an attacker would need to control, and subsequently estimate how much it would cost to purchase and/or rent.

3 Work term

The work term, W, is the cost associated with POW mining. The form of the work term is complicated by the availability of rental equipment, and so depends on market rental prices 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 of duration t_a, the rental costs are

$$R = a r_e t_a. \tag{6}$$

with the condition that $a \leq H_a$.

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 hardware. Devices will have a hashrate h_d, a power draw ω_d, and a retail cost p_d. The device can be modeled after a single state-of-the-art device, or parameters can be estimated based on a survey of market conditions and history. Modeling on the state-of-the-art device typically minimizes the cost, and is the method used here. If desired, an adjustment could be added to the retail price to account for support equipment, i.e. power supplies, networking hardware, etc.

Device parameters can also be 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 attacker's required hashrate, H_a, is related to the full network hashrate, H_{net}, through equation 4 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 (see appendix A).

$$H_{net} = \frac{\beta X}{\alpha_w \rho + 0.024 c/\eta} \tag{10}$$

where β is the total POW rewards (DCR) paid out daily. The benefit of parametrizing in terms of miner profitability is that the value is self-regulating and tends towards zero, allowing predictions of long-term behavior in a stable market. 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

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

with

$$H_a = \sigma(y) \frac{86400 s_w R_{tot} X}{t_b(\alpha_w \rho + 0.024 c/\eta)} \tag{14}$$

Equation 14 assumes units of seconds for block time and fiat/kWh for electricity rate.

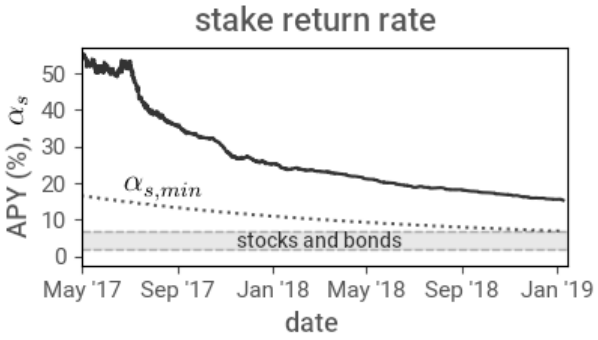

Figure 2: As Decred staking gains acceptance as an investment product, the returns are approaching those of other common investment products.

---

4 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.

Similar to the method used on 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, expressed as

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

with $R_{pos} = s_s R_{tot}$ (s_s is currently set at 0.3). Here again, a type of profitability is chosen for parametrization due to its tendency towards some natural value. APY in particular is chosen for convenience of comparison with other investment products. Contrary to equilibrium value of α_w, the asymptotic value of α_s is not zero. As shown in figure 2, as Decred staking gains acceptance as an institutional investment product, the return rate approaches 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 also a hard lower limit on the steady-state APY possible when $p_t = C(t)/Z$,

$$\alpha_{s,min} = \left[\frac{ZR_{pos}}{C(t)N} + 1 \right]^{365/28} - 1 \tag{17}$$

where $C(t)$ is the total Decred in circulation. This provides a lower limit to the valid range of α_s, illustrated as a dotted line in figure 2.

The stake term is expressed fully as

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

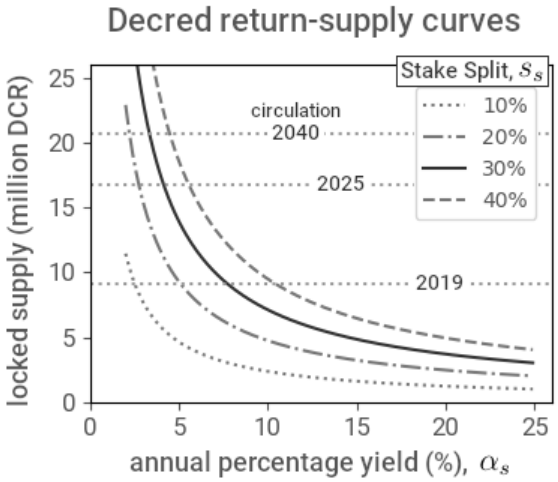

Figure 3: There is a lower limit to the steady-state APY where the total stake is equal to the total supply. The position of the limit can be modified by increasing or decreasing the fraction of the block reward given to ticket holders.

---

5 Application

To make use of the PCA, typically a starting position in parameter space is chosen, and parameters are varied one or two at a time around that position, treating all others as either constant, or changing in some known way with the chosen variable(s). For the sake of the following examples, the starting position is chosen to be the conditions at the time of writing ($X = 17.5, \alpha_s = 0.153, h = 309,000$), though the general trends are valid over a wide range of conditions. A cursory survey of rental mining equipment availabiity indicates a low rentability, $a/H_{net} < 0.01$. For the rest of this work, $a = 0$ will be used.

To demonstrate the application of the relations developed above, an attempt is made here to investigate a few common questions.

5.1 Which mining algorithm provides the highest network security?

At all but the highest rentabilities, the retail equipment term dominates the PCA. Using the relations developed in the appendix, it can be shown that at a given exchange rate, the retail capital, $C_{retail} = W/\sigma(y) = N_d \cdot p_d$, of devices on the network depends only on the price and power consumption of the device, and not on hashrate.

$$C_{retail} = \frac{Qp_d}{\alpha_w p_d + 0.024\omega_d c} \tag{19}$$

At high profitabilities, $\alpha_w p_t \gg 0.024 c w_d$, the device-dependence disappears completely.

$$C_{retail} \approx \frac{Q}{\alpha_w} \tag{20}$$

From a network security standpoint, the low-profitability condition is more relavent, as it represents a "steady-state" equilibrium condition that persists in the absense of market fluctuations or advancements in hashing hardware.

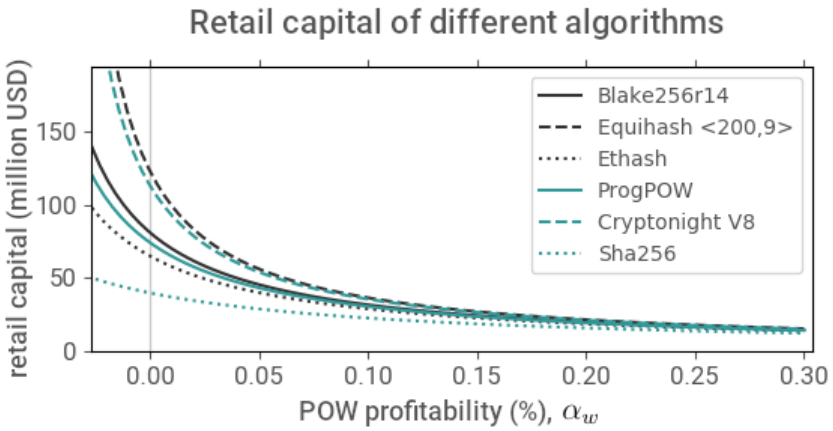

Figure 4: The difference in PCA between mining algorithms is more significant at low profitabilities. Those algorithms that maximize p_d/ω_d have higher PCA across the range of profitabilities.

There is a minimum profitability given in the zero-gross limit of equation 25,

$$\alpha_{w,min} = -\frac{0.024c}{\eta\rho} \tag{21}$$

which is an asymptote for $C_{retail}(\alpha_w)$.

At the time of writing, Decred mining profitability is less than zero ($\alpha_w = -2.7 \times 10^{-4}$), resulting in a PCA higher than the "steady-state" condition. This is the ideal state for a blockchain, as the PCA is higher than even the zero-profitability condition. It also indicates a good short-term outlook among miners, as the only way to recoup electricity expenditures is if the exchange rate goes up.

Maximizing the device factor, $p_d/\omega_d = \eta\rho$, can raise the PCA, as well as the minimum profitability. Further investigation may seek mining algorithms or alternative consensus mechanisms which can use more hardware but less power.

5.2 What is the best split of the block reward?

Transient behavior associated with an abrupt change to a blockchain parameter would be difficult to predict. Long-term behavior in a stable market is easier. If we stick to the assumptions layed out so far about mining profitability and stake returns, then "steady-state" conditions can be predicted.

The stake split, s_s, of R_{tot} imposes conditions on the treasury split, s_t, and the miner split, s_w, by the relation $s_t + s_s + s_w = 1$. The treasury split is left at 0.1 here. It is tempting to vary s_s, and consequently s_w, and minimize $A(y)$ on $[0, 1]$ at every point along the way, but that approach ignores nuanced economics that would occur if the attacker attempted to purchase a large portion of the ticket pool. How this would affect the stake difficulty can be predicted, but this action would also presumably spike the exchange rate as the attacker purchased Decred from exchanges to spend on tickets. The variation of X with y at high-y is harder to predict. In short, there is more confidence in low-y predictions than in predictions of the high-y region. Low-y conditions also require less time investment from an attacker, as acquiring a significant portion of the stake pool would require a lengthy ticket-buying campaign.

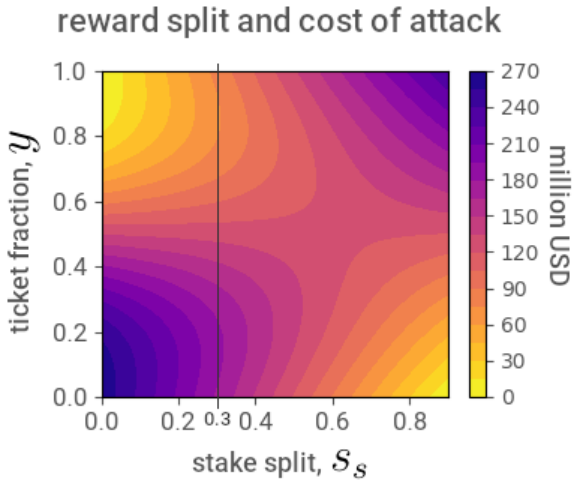

Figure 5: The PCA varies with stake split (fraction of block reward given to ticket holders) and stake ownership (portion of ticket pool under attacker control). All other parameters are network parameters on January 15th, 2019.

Figure 5 shows the variation of attack cost with y and s_s, in the zero-rentability case. The current network configuration of $s_s = 0.3$ is a good balance between high entry point at low-y, and gradual dropoff at $y > 0.5$.

5.3 Is Decred more secure than a pure proof-of-work blockchain?

Noting that $W \propto R_{pow}X$, we premise the comparison to a pure-POW blockchain on the equivalence of the fiat-converted inflationary rate,

$$\frac{R_{tot}X}{t_b} = \frac{R_{tot,pow}X_{pow}}{t_{b,pow}} \tag{22}$$

with appropriate considerations for the treasury split. Setting $S \to 0$, $s_w \to (1 - s_t)$, and $\sigma \to 0.5$ results in the pure-POW analogue of the PCA (here at zero-rentability),

$$A_{pow} = \frac{(1 - s_t)Q}{2(\alpha_w + 0.024c/\eta\rho)} \tag{23}$$

or alternatively,

$$A_{pow} = \frac{1 - s_t}{2s_w}A(0) \tag{24}$$

For an attacker with zero ticket fraction, the Decred consensus mechanism provides a boost of $2s_w/(1 - s_t)$ to PCA. With current network configuration, the boost is 4/3, or a 33% increase over pure-POW. As shown in figure 6, $A(y <\sim 0.25) \geq A(0)$, so an attacker would have to purchase about a quarter of the ticket pool to see any reduction in PCA.

The ticket fraction at which the hybrid PCA falls below the pure-POW PCA is found at the point $A(y_{eq}) = A_{pow}$. Decred currently has a y_{eq} of about 0.48, so an attacker would need to control about half the ticket pool to get the PCA below the pure-POW level.

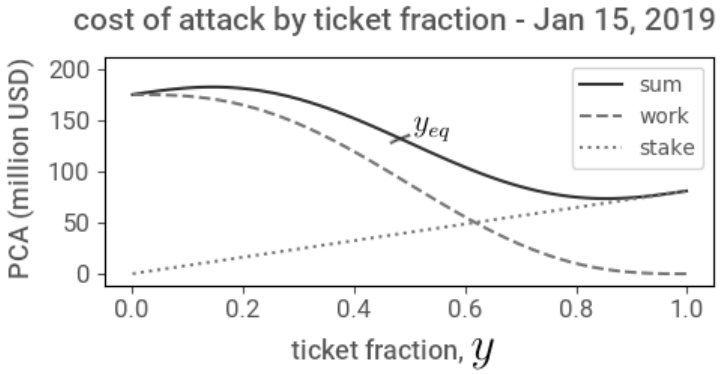

Figure 6: With increasing ticket fraction, the PCA shifts from work dominated to stake dominated. At point y_{eq}, the PCA is equal to that of a pure-POW blockchain with matching rate of fiat-converted inflation.

Appendices

A Network hashrate and POW profitability

Miner net daily earnings can be written as

$$E_{net} = \alpha_w p_d = \underbrace{E_g}_{\text{gross profit}} - \underbrace{\frac{24\omega_d c}{1000}}_{\text{power costs}} \tag{25}$$

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 presumably turn off their equipment and it will tend back towards zero.

The total fiat-converted value of block reward paid to miners daily, Q, depends on network parameters and the fiat exchange rate, X as

$$Q = \beta X \tag{26}$$

$$\beta = \frac{86400 R_{pow}}{t_b} \tag{27}$$

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

$$N_d = \frac{Q}{E_g} = \frac{H_{net}}{h_d} \tag{28}$$

Combining this relation with equation 25, and substituting alternative device parameters ρ and η, yields an expression for network hashrate.

$$H_{net} = \frac{\beta X}{\alpha_w \rho + 0.024 c/\eta} \tag{29}$$

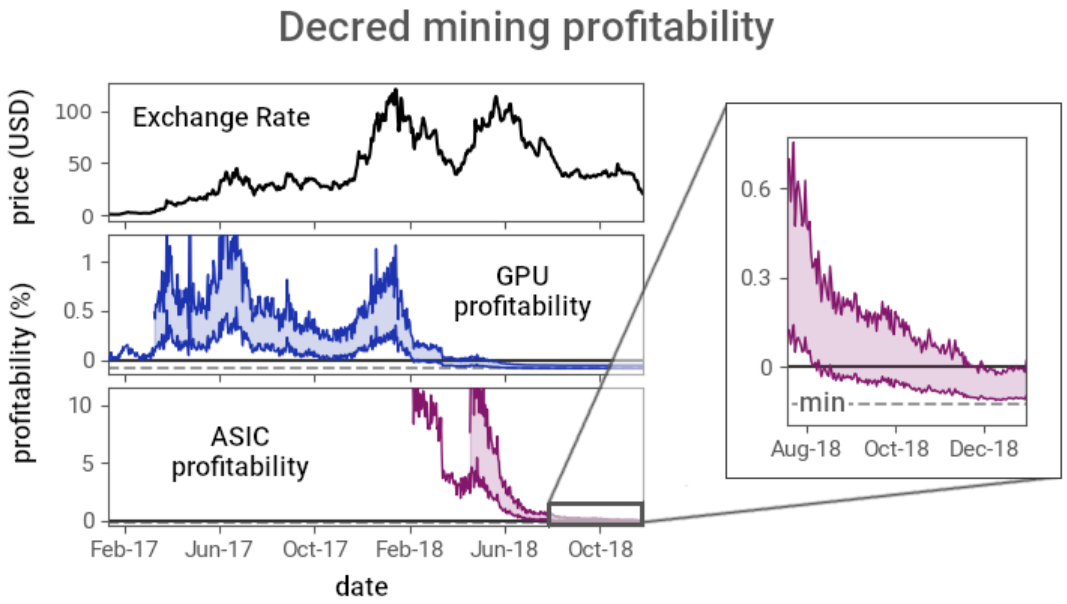

Figure 7: Mining profitability shows immediate response to price spikes, followed by decay towards zero when the price is stable.

The retail capital, C_{retail}, is the total retail value of all devices mining on the network, and is given by $C_{retail} = N_d p_d = H_{net}\rho$. The retail capital is the basis for calculating the retail terms of the PCA.

$$\frac{t_b}{P(y)} \tag{30}$$

$$\frac{t_b}{P(y)\sigma(y)} \tag{31}$$

	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 7.

algorithm	**Example**	**model device**	**price**	**hashrate**	**power**
$Blake256$	Decred	D9 Miner	1699	2.1×10^{12}	900
$CryptonightV8$	XMR	1080 Ti	475	950	180
$Equihash(200, 9)$	ZEC	Z9	475	41,000	3300
$Ethash$	ETH	Antminer E3	1150	1.9×10^8	760
$ProgPOW$	BCI	1080 Ti	475	2.2e7	275
$SHA256$	BTC	Antminer S15	1475	2.8×10^{13}	1596

Table 2: Model devices for mining algortihms used in section 5.2.

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.
C_{retail}	fiat	Retail capital. Total value of all devices mining on the network.
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	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.
s_t	–	Treasury reward share. Fraction of R_{tot} given as a to the Decred treasury.
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.
y	–	Attacker controlled fraction of the total stake pool.
Z	tickets	Ticket pool size. A network parameter.