REPORT FOR DASH DECENTRALISED GOVERNANCE ATTACK SIMULATOR

FILES TO BE GENERATED

test.csv, test.html, test.pdf

VALUES PROCEEDING WITH

Attack budget (£): 1000000.0 (user defined value)
Dash price (£): 50.0 (user defined value)
Inflation rate: 4.53 (user defined value)
Coins in circulation: 10000000 (user defined value)
Total of honest masternodes: 5000 (user defined value)
Honest masternodes already under control or bribe: 100
Target total masternodes: 20 (capped due to budget)
Total masternodes including already controlled or bribed: 120
Masternode block reward: 5.0DASH

ATTACK PHASE ONE: PRE-PURCHASE ANALYSIS

Active masternodes before purchase: 5000
Masternodes required for net 10% over honest: 5501
Attack budget (£): 1000000.0 (enough to acquire 20 masternodes)
Therefore, target total masternodes: 20
Excluding those already under control or bribe, total: 100
Finalised total of masternodes to acquire: 20

Coins in circulation before purchase: 10000000
From which coins frozen for required collateral: 5000000
Therefore, coins remaining available to acquire: 5000000
These are enough for this number of masternodes: 5000
Which as percentage out of the total possible masternodes is: 50.0%

ATTACK PHASE TWO: EXECUTION

FIRST PURCHASE ATTEMPT FOR 20 MASTERNODES

PURCHASE OUTCOME: POSSIBLE

HYPOTHETICAL REALISATION

Dash price before attack initiation (£): 50.0
Estimated Dash price after purchase (£): 50.91
Estimated total cost with inflation (£): 1000001.816
Therefore remaining budget equals (£): -1.816

Coins in circulation after purchase: 10000000
From which coins frozen for required collateral: 5020000
Therefore, coins remaining available to acquire: 4980000
These are enough to acquire more masternodes, specifically: 4980
Which as percentage takes this share from total possible masternodes: 49.8
However, 55% guarantees success in any governance attack
Theoretical total active masternodes after purchase: 5020
From which malicious: 20 + 100 = 120 (2.39% of total masternodes)

RETURN ON INVESTMENT

Money invested in this attack are not lost, just exchanged from GBP to Dash.
Daily Dash expected from masternode block reward: 75.0 (£3818.25)
Monthly Dash expected from masternode block reward: 2275.5 (£115845.7)
Yearly Dash expected from masternode block reward: 27375.0 (£1393661.25)
Estimated profits should also take into consideration any potential increase in the highly volatile original coin price with which masternodes were acquired.

SUMMARY

Number of masternodes required for malicious majority: 5501
The available coin supply was enough to buy this amount of masternodes: 5000

Estimated cost of maximum possible masternodes (5000) (£): 817499008.583

The attempted purchase was for: 20 masternodes
Estimated total cost with inflation (£): 1000001.816
Total active masternodes after purchase: 5020
From which malicious: 120 (2.39% of total masternodes)

INSIGHTS: WHAT PROBLEMS CAN WE CAUSE RIGHT NOW?

(1) PREVENT HONEST PROPOSALS TO GO THROUGH

EXAMPLE

Monthly salary of Dash Core Developers or other beneficial investments.

DESIGN VULNERABILITY

Proposals are not partially funded and remaining governance funds are burnt. Therefore, if attacked proposal is not in top rankings, it will be rejected.

SUCCESS LIKELIHOOD: HIGH

Because even if net 10% is achieved there is no funding guarantee. Funding is granted to the top X proposals based on net percentage.

METHODOLOGY

By down-voting proposals so that the net 10% margin is not achieved.

EXPLOITATION

Total votes of malicious masternodes: 20
Least honest votes required for net majority: 522
Maximum malicious masternodes based on available circulation: 5000
Least honest votes required for net majority: 5501

(2) MALICIOUS PROPOSAL PASSES BY NEGLIGENCE

EXAMPLE

Malicious proposal up-voted from malicious masternodes and abstention is high.

DESIGN VULNERABILITY

Votes are never questioned therefore if a proposal is accepted, no censorship exists.

SUCCESS LIKELIHOOD: MEDIUM

The controversy of a malicious proposal is expected to unite honest owners.

METHODOLOGY

Malicious proposal starts to be up-voted as close as possible to the closing window

EXPLOITATION

Total votes of malicious masternodes: 20
Least honest votes required for rejection: 0
Maximum malicious masternodes based on available circulation: 5000
Least votes required for net majority against maximum malicious: 0

HISTORIC DATA

Maximum votes ever recorded for funding a proposal is: 2147
At the time, this as percentage towards total masternodes was: 44.44%
Assuming a higher percentage this time due to unity from controversy: 60%
Which equals this number of honest masternodes: 3000

Therefore, total malicious masternodes needed for net majority: 3302

INFORMATION FOR THE FUTURE

Percentage of current circulation against total ever: 52.9%
Total ever coin supply: 18900000
Remaining ever coin supply: 8900000
Corresponding masternodes: 8900

EXPECTED CIRCULATION PER YEAR

09/2020: 9486800 (50.14% of total ever)
Available masternodes: -514

09/2021:10160671 (53.7% of total ever)
Available masternodes: 160

08/2029 (74.41%), 03/2043 (90.23%), 05/2073 (98.86%), 04/2150 (100%)