

## REPORT FOR DASH DECENTRALISED GOVERNANCE ATTACK SIMULATOR

### FILES TO BE GENERATED

dash-default.csv, dash-default.html, dash-default.pdf

### VALUES PROCEEDING WITH

Attack budget (£): unspecified (cost estimated in attack phase two)  
Dash price (£): 91.38 (real time value)  
Inflation rate: 2.26 (default exponential)  
Coins in circulation: 8789883 (real time value)  
Total of honest masternodes: 4860 (real time value)  
Honest masternodes already under control or bribe: 0  
Target total masternodes: unspecified (defaults to net 10% over honest)

### ATTACK PHASE ONE: PRE-PURCHASE ANALYSIS

Active masternodes before purchase: 4860  
Masternodes required for net 10% over honest: 5347  
Attack budget (£): cost of realise target of 5347 masternodes  
Therefore, target total masternodes: 5347  
Excluding those already under control or bribe, total: 0  
Finalised total of masternodes to acquire: 5347  
  
Coins in circulation before purchase: 8789883  
From which coins frozen for required collateral: 4860000  
Therefore, coins remaining available to acquire: 3929883  
These are enough for this number of masternodes: 3929  
Which as percentage out of the total possible masternodes is: 44.7%

### ATTACK PHASE TWO: EXECUTION

#### FIRST PURCHASE ATTEMPT FOR 5347 MASTERNODES

PURCHASE OUTCOME: IMPOSSIBLE

#### REASON

Because the remaining coins in circulation are not enough for 5347 masternodes but for a maximum of 3929, still capable for an effective cyber sabotage

### HYPOTHETICAL REALISATION

Dash price before attack initiation (£): 91.38  
Estimated Dash price after purchase (£): 103.47  
Estimated total cost with inflation (£): 520920725.108  
  
Coins in circulation after purchase: 8789883  
From which coins frozen for required collateral: 10207000 <--- (Problematic metric)  
Therefore, coins remaining available to acquire: -1417117 <--- (Problematic metric)  
Theoretical total active masternodes after purchase: 10207  
From which malicious: 5347 (52.3% of total masternodes)

### SUMMARY

Number of masternodes required for malicious majority: 5347  
The available coin supply was enough to buy this amount of masternodes: 3929  
The attempted purchase was for: 5347 masternodes <--- (Problematic metric)

#### SECOND PURCHASE ATTEMPT FOR 3929 MASTER NODES

PURCHASE OUTCOME POSSIBLE

#### ANALYSIS

Dash price before attack initiation (£): 91.38  
Estimated Dash price after purchase (£): 100.26

Estimated total cost with inflation (£): 376478414.446

Coins in circulation after purchase: 8789883  
From which coins frozen for required collateral: 8789000  
Therefore, coins remaining available to acquire: 883  
Total active masternodes after purchase: 8789  
From which malicious: 3929 (44.7% of total masternodes)

## SUMMARY

Number of masternodes required for malicious majority: 5347  
Available supply was enough for this amount of masternodes: 3929  
Estimated total cost with inflation (£): 376478414.446  
Total active masternodes after purchase: 8789  
From which malicious: 3929 (44.7% 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

Maximum malicious masternodes based on available circulation: 3929  
Least honest votes required for net majority: 4323

### (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

Maximum malicious masternodes based on available circulation: 3929  
Least votes required for net majority against maximum malicious: 3570

## 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: 2916  
Therefore, total malicious masternodes needed for net majority: 3209

#### INFORMATION FOR THE FUTURE

Percentage of current circulation against total ever: 46.5%  
Total ever coin supply: 18900000  
Remaining ever coin supply: 10110117  
Corresponding masternodes: 10110

#### EXPECTED CIRCULATION PER YEAR

09/2020: 9486800 (50.14% of total ever)  
Available masternodes: 696

09/2021: 10160671 (53.7% of total ever)  
Available masternodes: 1370

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