Raven Dark: An Open & Secure Privacy Blockchain

admin@raven-dark.com
www.raven-dark.com

Abstract: Most legitimate blockchain projects focus on a few, but not all, of the following features: Ubiquity, Openness, Privacy, Security and Fairness. Ubiquity has to be earned, but security, privacy, openness and fairness are core tenets. Raven Dark aims to incorporate all these core tenets with the goal of earning ubiquity.

1. The Core Tenets

Openness. Raven Dark aims to provide as much information about goals, projects, funds and technology as is possible without compromising security. As such, we'll be providing periodic reports on funding and goals as well as incremental technical white papers on projects.

Privacy. While we value openness in technology and in disclosing motives, we believe that people have the right to financial privacy if they wish. As such, the Raven Dark protocol provides means to privately send funds from one party to another.

Security. The Raven Dark team is committed to building and providing access to a secure blockchain platform and tools for interacting with the Raven Dark network, as well as other blockchain networks. We have the benefit of being built on top of the Dash codebase and hence are able to incorporate future security updates quickly.

Fairness. Raven Dark chose the x16r hashing algorithm so that individuals can use GPUs to mine and support the network. This was a deliberate decision as ASICs are seen as "unfair" to individuals due to their high costs and limited profitability window. Raven Dark will explore modifications to x16r or other algorithms if x16r ASICs choose to mine on the Raven Dark network.

2. Blockchain

I. *Core blockchain*

Raven Dark is built on the Dash codebase (once branded as Darkcoin) and therefore includes the majority of the Dash network's functionality and features, including: Masternodes [1], PrivateSend [2] and InstantSend [3]. The following sections detail modifications to the Dash codebase for Raven Dark.

II. *Supply*

The supply schedule has been modified to reflect the following specifications.
Total supply: 210,000,000
Block reward: 200 total, every 1 minute (85% PoW, 15% MN)
- 170 to PoW mining
- 30 to Masternode operators

Halving interval: 525600 blocks (~ 1 year)
Approximate future supply figures after:
1st year: 105,120,000
2nd year: 157,680,000
3rd year: 183,960,000
4th year: 197,100,000
5th year: 203,670,000

III. *Masternodes*

The required collateral and block reward have been modified to promote a reward schedule that is aimed being inclusive of individual miners and not over-rewarding masternodes. Collateral required to run a masternode is 50,000.

IV. *Difficulty algorithm*

A linear weighted moving average (LWMA) algorithm is used to compute difficulty for mining instead of Dash's Dark Gravity Wave algorithm. Raven Dark's implementation of the LWMA algorithm was devised by Zawy [4]. Difficulty is adjusted every 60 blocks and takes into account the average of the previous 45 blocks.

V. *Hashing algorithm*

Raven Dark uses the x16r hashing algorithm originally devised by the Ravencoin team [5]. This algorithm was chosen for its ASIC resistance and ability to be modified to continue ASIC resistance.

REFERENCES

[1] https://github.com/dashpay/dash/wiki/Whitepaper#2-masternode-network
[2] https://github.com/dashpay/dash/wiki/Whitepaper#3-privatesend
[3] https://github.com/dashpay/dash/wiki/Whitepaper#4-instant-transactions-via-instantsend
[4] https://github.com/zawy12/difficulty-algorithms/issues/3#issuecomment-442129791
[5] https://ravencoin.org/assets/documents/X16R-Whitepaper.pdf