Features Paper

MASTERNODES

Version 1.0 - May 2019

CONTENTS

Chapter 1

CHAPTER 1

Masternode Network

1. Introduction

A masternode is a full node running on a P2P network that allows peers to use them to send and/or receive information about events that occur on the network.

35%

Masternodes are rewarded 35% of each block reward for the services they provide to the network. Masternodes rewards are also effected by the Dynamic Reward System therefore making their rewards dynamic also.

Masternodes are very important to the health of the Zyrk network. They provide clients, peers and users the ability to synchronize and facilitate quick messaging over the Zyrk network. Masternodes should have high availability and provide a regular level of service to be eligible for rewards.

To run a Masternode the operator must provide proof of control of 7,500 ZYRK. Once provided these funds are marked unspendable while the Masternode is active.

While active the Masternode will provide services to clients, peers and users. Like miners Masternodes are also paid for these services - 35% of each block is dedicated as payment for these services.

Masternode rewards are also effected by the Dynamic Reward System (DRS) therefore making block rewards dynamic also. Due to the fact the Masternode rewards are a fixed percentage yet the amount of Masternodes fluctuate day to day the expected time of reward will vary day to day. Rewards for a standard day of operating a Masternode can be calculated using the following formula. Please note this assumes 100% uptime of your Masternode.

$$(n / t) * r\ b\ a$$

Where:
n is the number of masternodes owned
t is the total number of masternodes
r is the current block reward (DRS)
b is blocks in an average day.
a is the average masternode payment

There are also a limit of the amount of Masternodes active possible, due to the requirement to hold 7,500 ZYRK per Masternode.

This limit is calcualted by dividing the total available supply by 7,500 which will give the total amount of Masternodes possible at that time.

2. Determing which Masternode

A special algorithm is used to create a random ordering of Masternodes. To ensure secuirity of this algorithm the hash generated from the proof-of-work for each block is used. The example code below can also be extended further to provide the rankings and also rewards, it can also be extended by adding a 'second', 'third', 'forth' Masternode into the list.

```
For(mastenode in masternodes){
   current_score = masternode.CalculateScore();

   if(current_score > best_score){
      best_score = current_score;
      winning_node = masternode;
   }
}

CMasterNode::CalculateScore(){
  pow_hash = GetProofOfWorkHash(nBlockHeight);
  pow_hash_hash = Hash(pow_hash);
  difference = abs(pow_hash_hash - masternode_vin);
  return difference;
}
```

3. Role

Masternodes can provide an unlimited amount of extra services, eventually being able to pick and choose which services they wish to provide.

65%

Average amount of total supply of Zyrk locked for use as Masternode collateral. Over half the Zyrk network is dedicated to providing these extra features.

3.1. Zyop

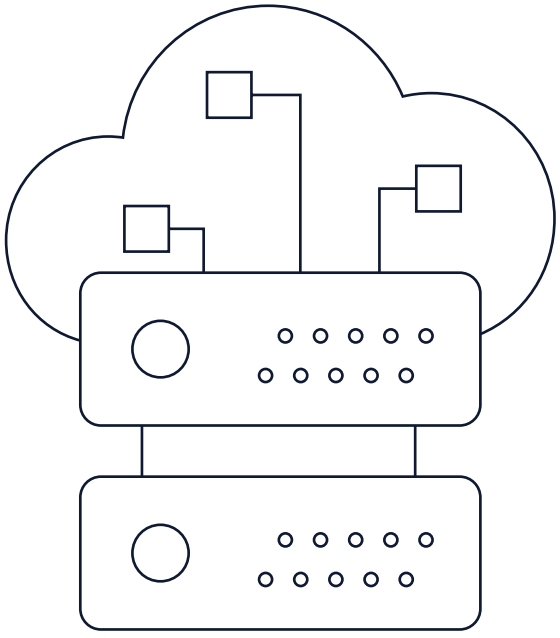
Masternodes can provide any number of extra services to the network. The Masternode service platform is one of our main areas of focuse due to the decentralized, consensus and governance platform it provides. As a proof-of-concept our first addition will be an implementation of Zyop. Zyop is an attempt at implementing a trustless, private and secure protocol for transfering Zyrk.

Unlike Zerocoin, Zyop will remove the trusted setup, reduce proof sizing (5-10%) and feature improved security. You can read more about Zyop in our upcoming Technical Paper.

3.2. Malicious Users

Malicious users could also run a number of Masternodes themselves but not provide any of the services to users/peers. To reduce the possibility of people using the Masternode system to their own advantage every Masternode must 'ping' the rest of the network every 15-30 minutes to ensure they stay active. Two Masternodes are selected every block to check that they are still active, if they are not they are removed from the list and no longer provide services or gain rewards.

When a Masternode rejoins the network they are then put at the bottom of the 'score' list and will be lower priority for payment. This incentivises each Masternode to stay active and provide services. The selection of the Masternodes each block is completely random and you could be chosen multiple blocks in a row.



4. Masternode Protocol

4.1. Propagation

Masternodes are propagated around the network using a series of protocol extensions including a masternode announce message and masternode ping message. These two messages are all that is needed to make a node active on the network, beyond these there are other messages for executing a proof-of-service request, Zyop and Zyox that are currently in the works.

After a specific time has expired the network will remove an inactive node from the network, causing the node to not be used by clients or paid. Nodes can also ping the network constantly, but if they do not have their ports open, they will eventually be flagged as inactive and not be paid.

New Masternodes entering the Zyrk network must be made aware of the currently active masternodes on the network to be able to utilize their services. As soon as they join the mesh network, a command is sent to their peers asking for the known list of masternodes. A cache object is used for clients to record masternodes and their current status, so when clients restart they will simply load this file rather than asking for the full list of masternodes.

4.2. Payments

To ensure that each masternode is paid its fair share of the block reward, the network must enforce that blocks pay the correct masternode. If a miner is non-compliant their blocks must be rejected by the network, otherwise cheating will be incentivized.

We propose a strategy where masternodes form quorums, select a winning masternode and broadcast their message. After N messages have been broadcast to select the same target payee, a consensus will be formed and that block in question will be required to pay that masternode.

5. Conclusion

This paper introduces various concepts to improve the design of bitcoin resulting in improved privacy and fungibility for the average user, less price volatility and quicker message propagation throughout the network. This is all accomplished by utilizing an incentivized two-tier model, rather than the existing single-tier model in other cryptocurrencies such as Bitcoin. By utilizing this alternative network design it becomes possible to add many types of services and develop on these in the future.

6. References

- https://github.com/zyrkproject/papers
- http://en.wikipedia.org/wiki/NIST_hash_function_competition#Finalists
- https://getaddr.bitnodes.io/nodes/incentive/
- http://research.microsoft.com/pubs/156072/bitcoin.pdf
- https://bitcoin.org/bitcoin.pdf

Zyrk Project

Masternode Paper

https://zyrk.io
team@zyrk.io

Revision 1.0 - May 2019