Zyrk Project

WHITEPAPER

Version 1.0 - May 2019

CONTENTS

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

CHAPTER 1

Introduction

1. Introduction to Zyrk

The creation of the Blockchain era occured in 2009 with the implementation of Bitcoin created by an entity known only as Satoshi Nakamoto. Following the huge success of Bitcoin gave rise to multiple competing crypto-currencies, Zyrk being one of them.

71%

of Bitcoin's network hashrate is based in China. Not only does this pose security issues but is a leading cause of centralization.

Bitcoin despite regular and constant innovation has unfortunately not been able to succeed in being widely adopted and accepted as a real world currency. It has nearly been a decade since the launch of Bitcoin but this lack of wide adoption has created a public view of Bitcoin being just a risky investment opportunity.

Zyrk aims to bridge this gap between the online realm and the real world. It strives to provide a safe, private and decentralized means which not only investors, but the general public can conduct business. Without the need for financial institutions or third parties Zyrk aims to provide everyone a fast, safe and private means to conduct business themselves.

1.1. Privacy

Privacy is an essential part of everyones day to day lives, why should finances be any different? The basis of Zyrk integrates Bitcoins greatest feat a distributed ledger consensus technology. Mixed with the speed and governance attributes from Dash such as Masternodes and governance related quorums. Finally the addition of our own Zyop protocol providing safe, secure and anonymity to all transactions whether mined or transacted Zyop covers all bases.

Zyop is the next addition to the Zyrk network and is currently under heavy development. Please read our 'Feature Paper' on Zyop to learn more about the technical intricacies.

1.2. Vision

The Zyrk project believes that everyone has the right to make their own choices and everyone should be allowed freedom, privacy and choice.

The world seems to ignore everyones request to privacy and freedom. The Zyrk project aims at allowing the general user to conduct business in a free and private way.

Users should also be given the choice on how they wish to conduct their business as long ago financial institutions started to dictate how, when and where the general public can or can't conduct business.

We want you to join the revolution and help shape Zyrk into the network that cannot and will not be stopped. Free, private, secure just how you want it.

CHAPTER 2

Overview

2. Overview

The Core developers of the Zyrk Project are long standing friends from an old programming IRC channel. With cryptography and the rise of Bitcoin ideas started to float around about the creation of Zyrk.

Research and discussions have taken place over the last 18 months and finally the release of the basis of the network now. The main motivation for the Zyrk project is to push the boundaries of technology that other well established projects are hesitant to do.

We strive for advanced features and technology and aim to create an eco-system to be built upon by us developers and end users. The Zyrk Project also aims to be self-supporting and decentralized while maintaining high security and anonymity.

The software technology behind Zyrk is from a line of successful cryptocurrencys, which each also tried to solve and improve upon issues before them. Zyrk originated as a fork of Dash, who forked from Litecoin, who forked from Bitcoin. These cryptocurrencies are all regarded as being in the top 10 of cryptocurrencies.

2.1. Fair Launch

The Zyrk network launched with fairness in mind. The first 250 blocks on the blockchain all reward 1 ZYRK. This was to stop the 'instant mining' of a brand new network and allow the news of our launch to travel. Roughly 6 hours was taken to mine these blocks allowing ample time for users to communicate, setup and spread the word of Zyrk before normal block rewards started and things got into full swing.

2.2. Self Supporting

With no pre sale or initial coin offerings Zyrk aims to be fully self sufficient and driven by the general public. On chain governance and budgeting systems allow users to dictate and allocate where funds are spent or not. Allowing you the user to voice your opinion and create your choice, whether it is anonymous or not is also up to you.

2.3. Specifications

Zyrk uses proof-of-work to secure and generate blocks. X16R is the hashing algorithm used for this proof-of-work. On average a block is generated/mined every 120 seconds and the difficulty is adjusted **every** block to ensure this time is kept. Block sizes are maximum 4MB and segwit addresses/transactions are enabled by default. There was no presale or initial coin offering but there was a small premine of 0.5% which aims to pay for development, server infustructure, any outsourced work (advertising/marketing) and future research and development. You can see a full list of specifications in a table below.

2.4. Dynamic Rewards System

Zyrk employs a Dynamic Reward System. Unlike native block rewards in the likes of Bitcoin or Litecoin where there is a fixed reward that then halves every x blocks. Each block is calculated based on the average network hashrate over the last **24** blocks. This is to ensure network fluctuations from outside sources (renting hash, pool hopping and purposely pushing hashrate up) is minimized due to the amount of time to get a higher average over 24 blocks. The rewards are laid out in a table below.

Blockchain Specifications

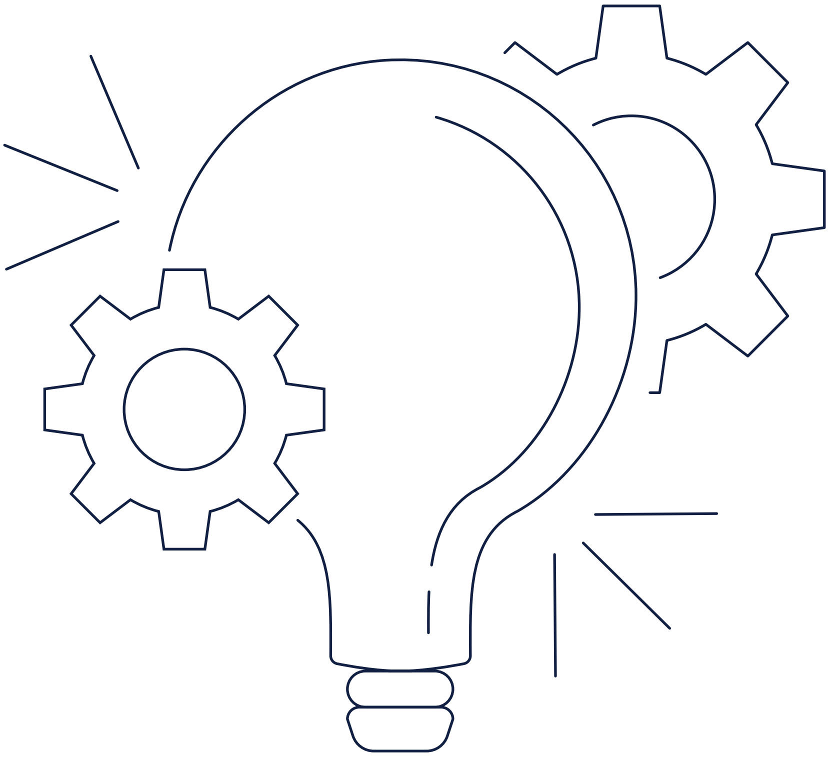
Algorithm	X16R
Ticker	ZYRK
Block Time	120 Seconds
Block Size	4 MB
Block Rewards	Dynamic (DRS)
Amount	25 - 125 ZYRK
Premine	0.5%
ICO/Presale	No

Masternodes

Collateral	**Reward**
7,500 ZYRK	35% of block

Dynamic Reward System

Network Hashrate	**Reward**
0 (GH/s)	25 ZYRK
5 (GH/s)	28 ZYRK
15 (GH/s)	35 ZYRK
25 (GH/s)	42 ZYRK
50 (GH/s)	50 ZYRK
100 (GH/s)	65 ZYRK
500 (GH/s)	80 ZYRK
1000 (GH/s)	95 ZYRK
5000 (GH/s)	110 ZYRK
20000 (GH/s)	125 ZYRK



> A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990’s. I hope it’s obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we’re trying a decentralized, non-trust-based system.
>
> Satoshi Nakamoto

CHAPTER 3

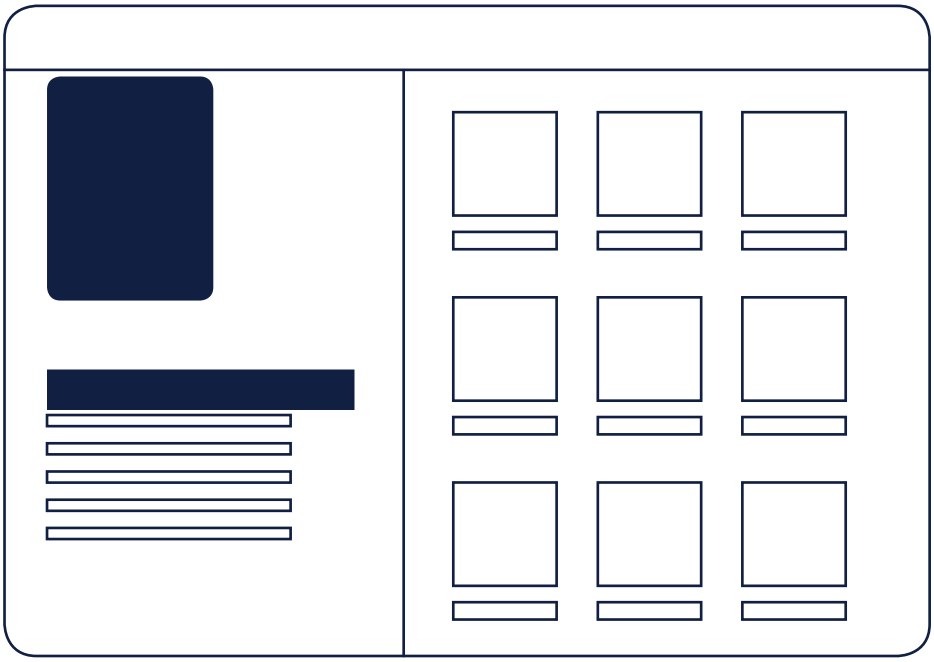
Masternodes

3. Masternode Network

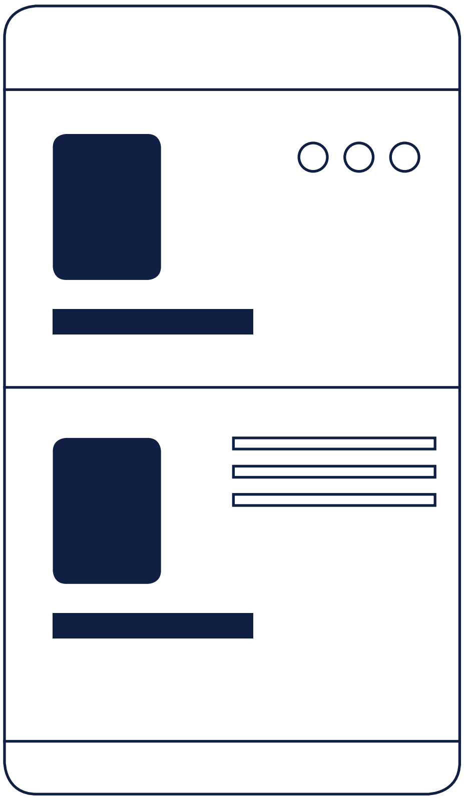
A masternode is a full node running on a P2P network that allows peers to use them to send and/or receive information about events that occur on the network.

3.1. Overview

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.



3.2. Rewards

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

$$(n/t)*rba$$

Where:

n is the number of masternodes owned

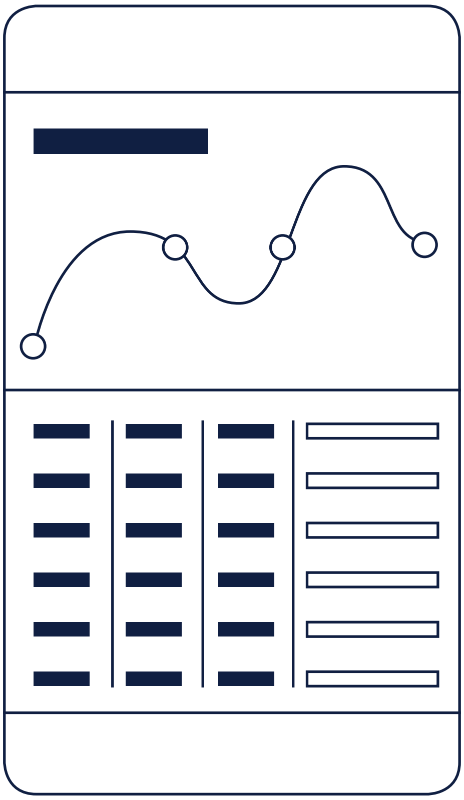
t is the total number of masternodes

r is the current block reward (DRS)

b is blocks in an average day.

a is the average masternode payment

```
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;
}
```



3.3. Roles

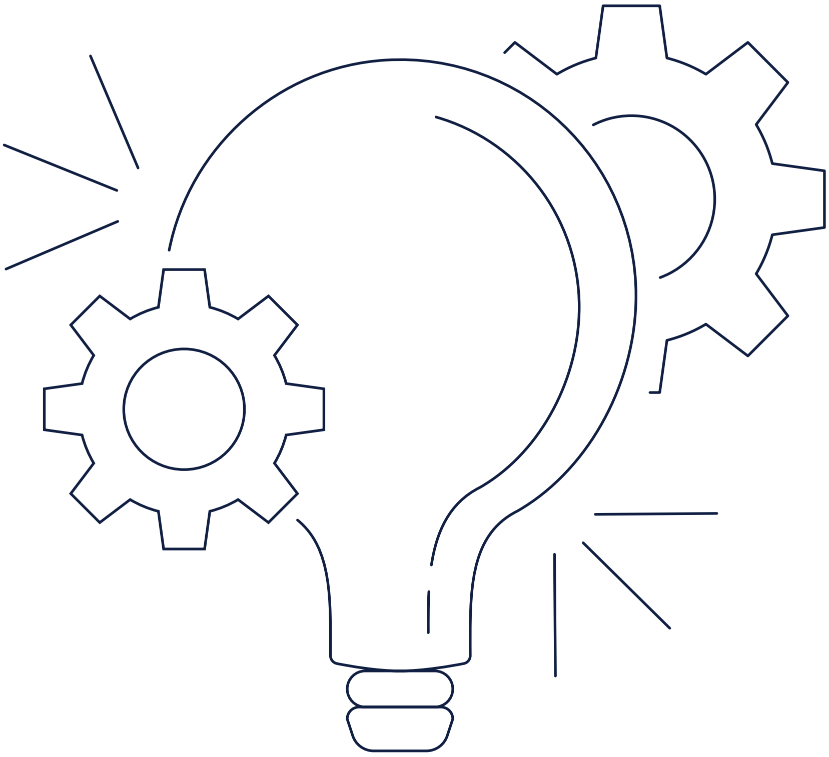
Masternodes can provide an unlimited amount of extra services, eventually being able to pick and choose which services they wish to provide

3.3.1. Zyop

Masternodes can provide any number of extra services to the network. The Masternode service platform is one of our main areas of focus 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 Features Paper.

3.3.2. 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



3.4. Protocol

3.4.1. Propogation

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

3.4.2. 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 would 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.

> **The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.**

Satoshi Nakamoto

CHAPTER 4

Zyop Technology

4

4.1 Abstract

It is proposed that Zyop a new pirvate and anonymous transaction system which ensures both transaction confidentiality and anonymity, small proof sizes, short verification times and **without requiring a trusted setup.** Inspired by the Zerocoin protocol, Zyop improves and adds to the original Zerocoin functionality to support private transactions while also greatly increasing in performance. Zyop proof sizes are almost 75% smaller compared to original Zerocoin proof sizes. Zyop builds on the techniques of Confidential Transactions, Zerocoin and Oneout-of-Many proofs and its efficiency is particularly well-suited for enabling private blockchain transactions with minimal trust required.

4.2 Overview

For cryptocurrency transactions to be truly private, transactions must have the following two properties;

1. Confidentiality (e.g hiding the transferred amounts)
2. Anonymity (e.g hiding the identity or identities of the sender and/or receiver of the transaction)

Bitcoin Core has introduced the concept of Confidential Transactions in which its design only the amounts are hidden from the general public view using a commitment to the amount transacted. The flaw in this design is that it does not ensure transaction anonymity, which is a highly desirable feature for financial transactions.

Although Zerocoin and Zerocash can offer this there are significant downsides. While Zerocoin does offer transactional anonymity it only works with fixed amount denominated coins and these amounts are also not hidden. Zerocash on the other hand is capable of hiding transaction values, their origins, and destinations it does come at a price though. The reliance on knowledge of exponent assumptions and a trusted setup process, necessitating the user's trust in the correctness of this setup.

Comparison to other Privacy Solutions

	Anon Set Size	Trusted Setup	Proof Size (KB)	Proof Time (s)	Verification Time (ms)
Monero	10	No	2.1	1	47
Zerocash	2^32	Yes	0.3	1-20	8
Zerocoin	10,000	Yes	25	0.2	200
Zyop	2^14	No	1.5	1.5	13

CHAPTER 5

The Team

Mykel Zhao

Lead Blockchain Developer

Mykel is the founding lead blockchain developer for the Zyrk Project. With a curious interest in Bitcoin since the release way back in 2009, Mykel has watched and participated in many network launches until the idea of Zyrk was created as a movement to change and improve on features he thought was missing in most competing cryptocurrencies.

Jackson Friel

Software Engineer

Jackson was recruited once development for Zyrk was already well underway, Jackson currently works part time on the project to give a helping hand to Mykel due to him just having a new born addition to his family. We hope to see more of Jackson over the coming years and potentially move in to a full time role.

Oscar Goodwin

Systems Admin/Analyst

Oscar was a bit late to the cryptocurrency world, only finding out about Bitcoin around the Mt Gox crash. Oscar has been a Systems Administrator and Analyst for a few high profile technology companies including a large scale hosting company. Oscar looks after all website, server and hosting related parts of the project.

Wayne Ahl

Cryptography Expert

Wayne has always had a eagerness to solve things, which lead him to cryptography. He first learnt of cryptography by subscribing to the Metzdowd mailing list around the time Satoshi released the first version of Bitcoin. Wayne is responsible for the creation of Zyop - making trustless, anyonymous and secure transactions.

Zyrk Project

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

Revision 1.0 - May 2019

Copyright 2019