

FOLMCOIN

# White Paper

03.2018 | V1.0



**Payment key  
for the future**  
secure and anonymous

# What's Happening

**Introduction**

**Philosophy**

**Features & Specifications**

**Crypto Algorithm**

**What's Next**

**About FolmBank**

**Blocks and Rewards**

**Masternodes**

**Mining and Pools**

**Roadmap**

**Downloads and Useful Links**

**Community**

# Introduction

FOLM coin was designed as a masternode-based payment system. Our team, has been reviewing developments in Blockchain technology over time and has also studied many blockchain-based cryptocurrencies and identified a number of deficiencies related to them. We wanted to create a new innovative and cutting-edge cryptocurrency that will make several improvements in Blockchain technology and address some of these deficiencies. We decided to create FOLM coin.

The FOLM infrastructure uses the codes that make up Bitcoin (Bitcoin Core). We have also combined some codes from Bulwark cryptocurrency, enriched with current great blockchain technologies, and for the first time with the crypto algorithm used in Luxcoin called PH11612. After a lot of debugging and development, we have worked on some improvements to ensure that miners will be able to mine without problems.

For example, the FOLM team has developed a special algorithm for detecting and adjusting mining difficulties, which is a major problem in mining. This algorithm detects the mining difficulty based on fluctuating hashpower using short block intervals and adjusts the difficulty levels using statistical data of the last few blocks found.

These and so many small but important developments have made it possible for FOLM coin to be one of the most seamless cryptocurrencies for both circulation and mass adoption.

# Hello.

# Philosophy

We needed to define FOLM coin briefly and have therefore defined it as a cryptocurrency that is at the intersection of performance and security. For example, the block length of Bitcoin is 1 MB, which causes delays in payment transfers. Where much longer blockchains have been proposed, the presence of larger sized blocks and the creation of orphan blocks threaten the reliability of the system. We have chosen a reasonable but not overly long block length (4MB) that would meet both transfer speed and system security.

**FOLM is a cryptocurrency that is at the intersection of performance and security.**

With the features of FOLM, we are aiming to become a safe payment system for the future as well as a problem-free structure that can serve as the backbone infrastructure for many blockchain projects.

In addition, we knew that the most important part of a cryptocurrency are the miners who secure the network and keep transactions flowing. We wanted to make sure that the new cryptocurrency will provide sustainable profits for miners and masternode holders. For this reason, block rewards, their distribution ratios and annual distribution ratios will be maintained. We believe that masternodes are a very important component of our system in particular.

Many Cryptocurrencies have seen a reduction in the emission rate in the years following initial release. This combined with the higher cost of creating a new Master-node once the coins value goes up leads to diminished use and depreciation in the years following initial release. Usage declines without the attractiveness of new coin rewards. To counter this, we aim to provide more incentives with the reward system in the second year than in the first year. This will incentivize masternode holders to stay longer while seeing themselves as business partners.

And last but not least the FOLM development team will continue to monitor developments in the blockchain technologies ecosystem and we promise to integrate original innovations into FOLM over time.

With its features, FOLM will be not only be today's cryptocurrency but also tomorrow's cryptocurrency.

# What's Next

Folm aims to be your future payment system. For that firstly, we have analyzed the problems that have been happening with existing blockchain-based coins and have decided to architect FOLM with good block time, block size and other great features for a seamless and sustainable blockchain infrastructure.

We have developed a payment system that will work on top of this infrastructure as a "SaaS" service, bringing innovative solutions to today's businesses and real life applications, solving a lot of problems, and most importantly, allowing you to easily develop a blockchain infrastructure without any forking.

We aim to be a modern payment solution that not only brings innovative solutions for payment solutions but also work for many years without problems.

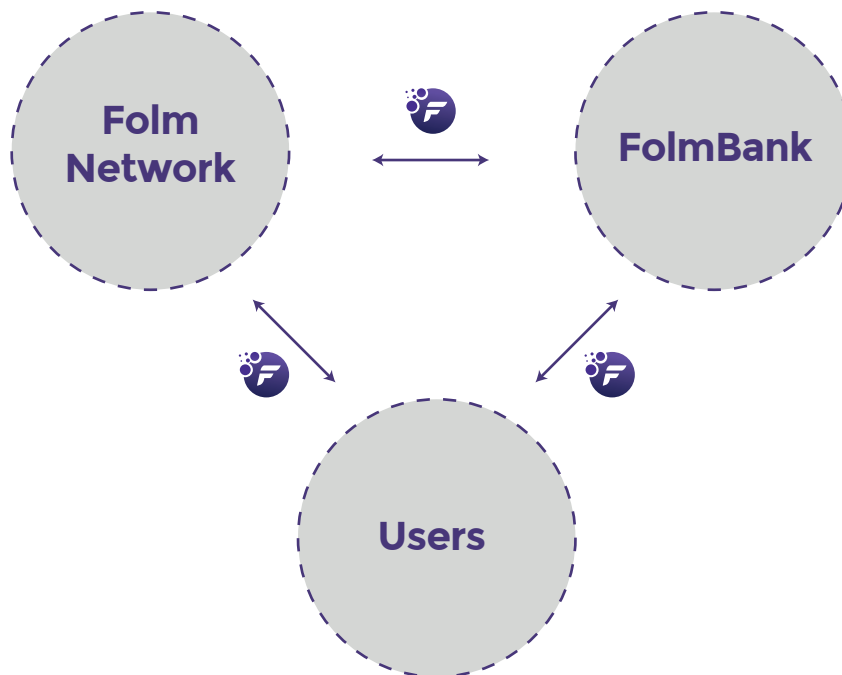
And we will introduce you to a brand new concept that has never seen before:

## FolmBank



# About FolmBank

The FOLM Bank is a SaaS (Solution as a Service) running on the FOLM network. Owners of FOLMs can make smart payment contracts on the FOLM Bank. Once the conditions of the contracts have prepared appropriately, they provide the required folm circulation on the blockchain.



FolmBank will provide great convenience with features you have never seen before. It has superiorities than former possibilities of the blockchain technology.

Users can ensure that a payment procedure is expendable with the approval of the paying party. Otherwise, even if the payment went to the opposite side, it will not be expendable (transferable to another party).

Users can create payment templates based on agreements between the parties involved. For example, User might create a payment template that divides jobs on a service contract and ensures that payment is released only if the relevant milestones are completed and the sender has granted the approval to release the funds.

The transfer of digital assets to legitimate heirs in case of death has always been a problem. With the Folm bank, users can automatically transfer all of their assets if user's legal heirs die. This will be made seamless and automated.

Users can send an expendable payment to a later date. For instance, User 1 paid User 2 now. However, User 2 can start spending 6 months later. Among these, the FOLM Bank will be the payment key for the future with many more features.

# Features & Specifications

Ticker	<b>FLM</b>
Algorithm	<b>PHI1612</b>
Blocktime	<b>120 seconds (2 minutes)</b>
Reward	<b>45 ( 30 POW + 15 MN )</b>
Block Confirms for Mined Blocks	<b>49 ( 98 Minutes )</b>
Block Confirms for Send/Receive	<b>10 ( 20 minutes )</b>
Block Maximum Size	<b>4 MB</b>
Maximum Coins	<b>23.001.916 (POW) (Included premine)</b>
Premine	<b>1.136.956 (%5 of POW)</b>
Halving	<b>Unique FOLM Supply Method for Every Year</b>
Default Port / RPC Port	<b>53656 / 53654</b>
Minimum Transaction Fee	<b>0,0001 FLM</b>



## Open Source and Decentralized

FOLM is a blockchain based coin which is open source and decentralized.



## Best Secure Algorithm

The PHI1612 algorithm is one of the most secure encryption algorithms, A combination of Skein, Jh, Cubehash, Fugue, Gost and Echo crypto algorithms.



## Purified Some Bugs of Blockchain

Purified Some Blockchain Bugs Most cryptocurrencies live with some bugs that may cause big problems in the future. FOLM identified and solved these problems before going live, delivering a stable blockchain.



## Instant Send

InstantSend is an advanced service that allows for near-instant transactions to take place. With this system, inputs can be locked to specific transactions and verified by consensus of the masternode network.





## Anonymous Send

Anonymous Send starts off by breaking your transaction inputs down into standard denominations. These denominations are 10000, 1000, 100, 10, 1 and 0.1 FLM – kind of like the paper money that you use every day.



## SlowStart

Our fair start is provided with the following code snippet (Credit: ZCash).



## Dark Gravity

Dark Gravity Wave, or 'DGW' works by adjusting the difficulty levels for every block by the checking last 20 blocks (instead of every 2016 blocks like Bitcoin), using statistical data of the last blocks found.



## Common Sensible Block Size

Block Size is designed as 4MB. This is 4x greater than Bitcoin's block size, while also having just 2 minutes block time which is 5x less than Bitcoin. In total FOLM is able to process 20x more transactions than Bitcoin.



## Unique and Profitable Reward System

FOLM is designed to provide optimal profits for miners and masternode holders. For this reason, it has been redesigned with a unique supply methodology instead of the classic method used in most cryptocurrencies.



## With Masternodes Earn While You Sleep

Owners of FOLM Masternodes, can earn high block rewards without mining.



## Mining with Less Energy and Heat







With our crypto algorithm, you can mine FOLM, with less energy and heat.

# Crypto Algorithm

Algorithms Comparison .....	11
Why Phi1612 .....	12
Phi1612 Algorithm .....	12

# Algorithms Comparison

Phi1612 Algorithm is a power friendly algorithm so you can mine efficiently.

GPU USAGE	SKEIN	PHI1612	NIST5	SKUNK	NEOSCRYPT	D.HASHIMOTO
GPU USAGE(MIN)	79	30	52	70	83	95
GPU USAGE(MAX)	99	101	111	106	108	101
GPU USAGE(GRAPH)						
NICEHASH	NO	NO	YES	YES	YES	YES

Also Phi1612 can work efficiently with Nvidia and AMD GPUs.



Nvidia Miner



Amd Miner

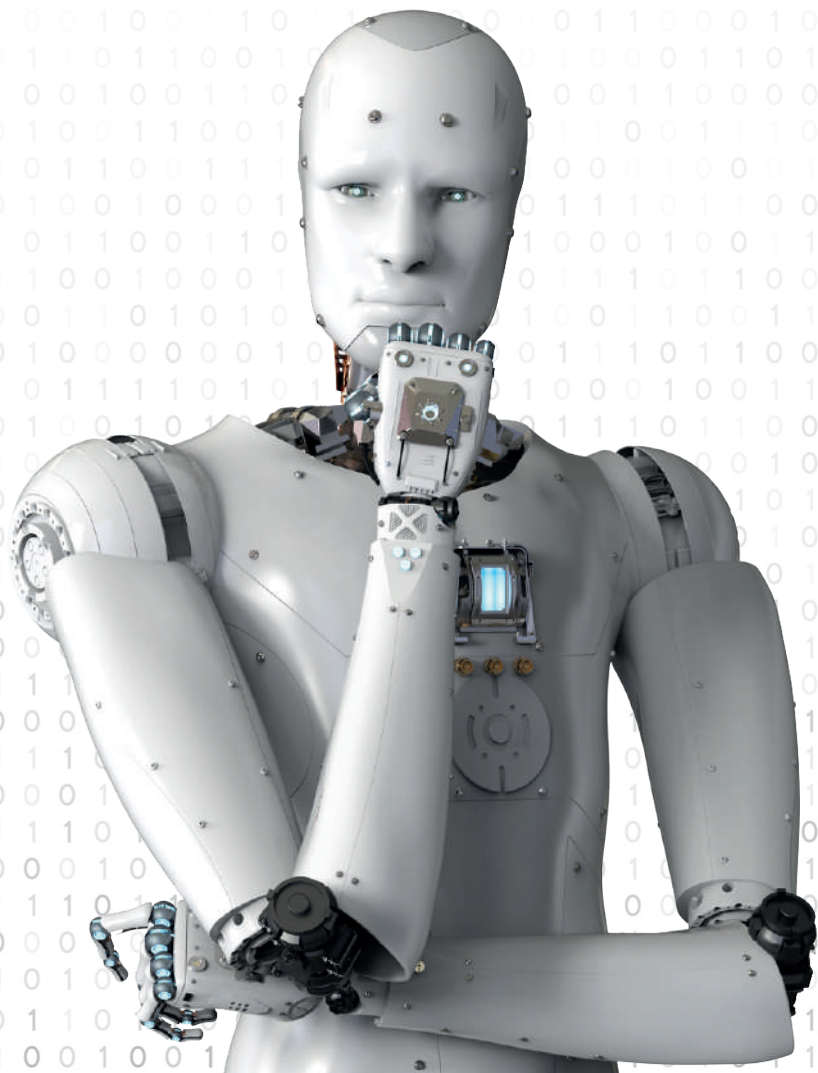
# Why Phi1612

Released by 216k155 with Luxcoin, The PHI1612 algorithm is one of the most secure encryption algorithms; combination of Skein, Jh, Cubehash, Fugue, Gost and Echo crypto algorithms. It does a GPU-based calculation during encryption. Unlike the other encryption algorithms, GPU resources are not always used at the highest level during mixed encryption calculations. This means there will be less electricity consumption and less heat generation. Thus, it has a resource-friendly approach and does not compromise security. Phi1612 can be mined on a wide array of consumer-grade hardware including CPUs, as well as AMD and NVidia GPUs. Phi1612 is ASIC and Nicehash resistant.

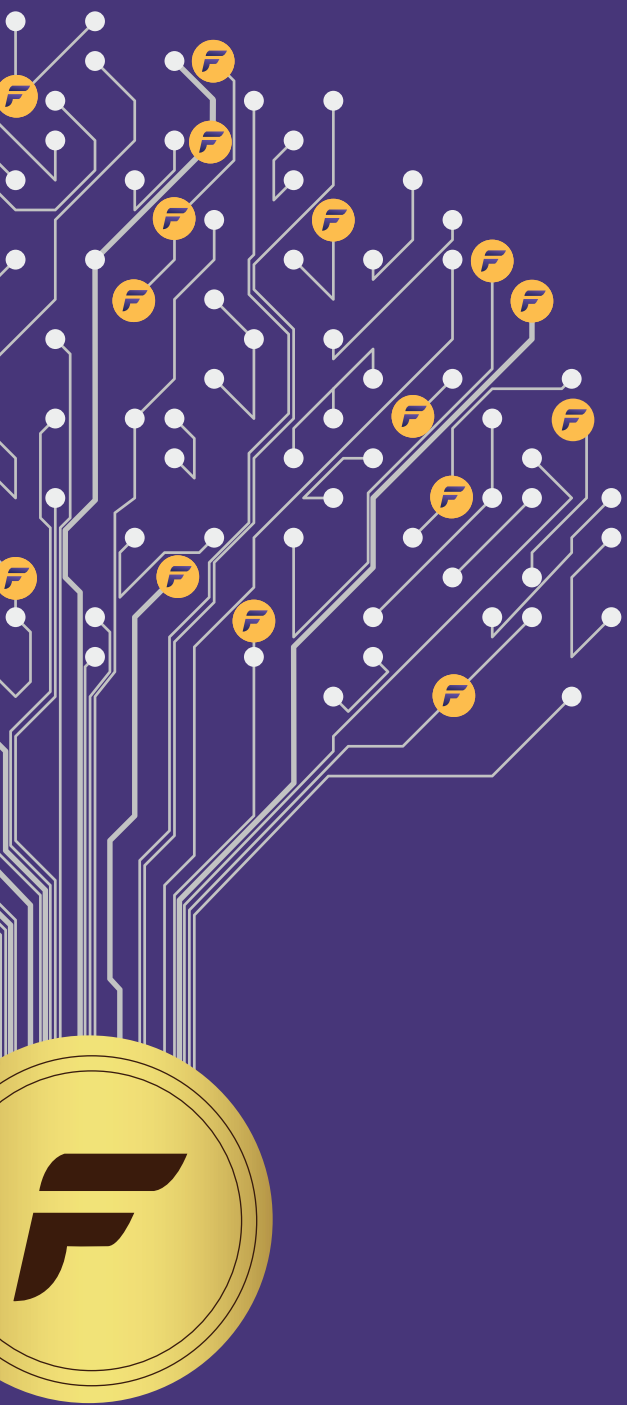
# Phi1612 Algorithm

The six hashing algorithms that make up Phi1612 are:

Cubehash (Daniel J. Bernstein 2009), Echo (Petri Nets 2012), Fugue (Shai Halevi, William E. Hall, and Charanjit S. Jutla 2019), Gost (RF. 2012), Jh (Wu 2012), and Skein (Ferguson et al. 2010)



# Blocks and Rewards



<b>At a Glance</b>	.....	14
<b>Block Rewards</b>	.....	14
<b>Proof of Work (PoW)</b>	.....	15
<b>Coin Distribution</b>	.....	16
<b>Premine</b>	.....	17

# At a Glance

Our block size and time, designed for best performance and security.

Blocktime	<b>120 seconds (2 minutes)</b>
Reward	<b>45 ( 30 POW + 15 MN )</b>
Block Confirms for Mined Blocks	<b>49 ( 98 Minutes )</b>
Block Confirms for Send/Receive	<b>10 ( 20 minutes )</b>
Block Maximum Size	<b>4 MB</b>
Total Coins ( POW + POS )	<b>54.045.121,00 FLM</b>

## Block Rewards

Today most cryptocurrencies yield a very high ROI in the first year. However, in the following years, this gain is reduced, while the bonus rewards per block is reduced. Instead of this, FOLM increases the number of block masternode prizes in the second year, thus making masternodes win more.

	POW	MN	TOTAL
1. Year	30+ Fee/2	15+ Fee/2	45+ Fee
2. Year	20+ Fee/2	20+ Fee/2	40+ Fee
3. Year	10+ Fee/2	15+ Fee/2	25+ Fee
4. Year	5+ Fee/2	10+ Fee/2	15+ Fee
5. Year	2,5+ Fee/2	7,5+ Fee/2	10+ Fee

# Proof of Work (PoW):

Proof of Work (PoW) as the name states is the validation of the work that happened and proving it is correct. Bitcoin and many alt coins follow this way of consensus to make sure of the authenticity of the chain.

To understand how it works in simple terms, assume that you are in a math exam along with other students in a classroom. The student who can, not only come up with the correct answer but also can come up with the complete proof (steps in math terms) of arriving at the correct answer first gets the reward. As we know this requires a student with a lot of brain power which will naturally consume a lot of energy from the body.

Now mapping it to the cryptocurrency world, "math exam" refers to the "transaction", the "classroom" refers to the "world", "Student" refers to the "computing hardware/computer" that runs the complex algorithms, "brain power" refers to the "computing power" and the "lot of energy" refers to the "lot of electric power". I hope it is easier now to understand.

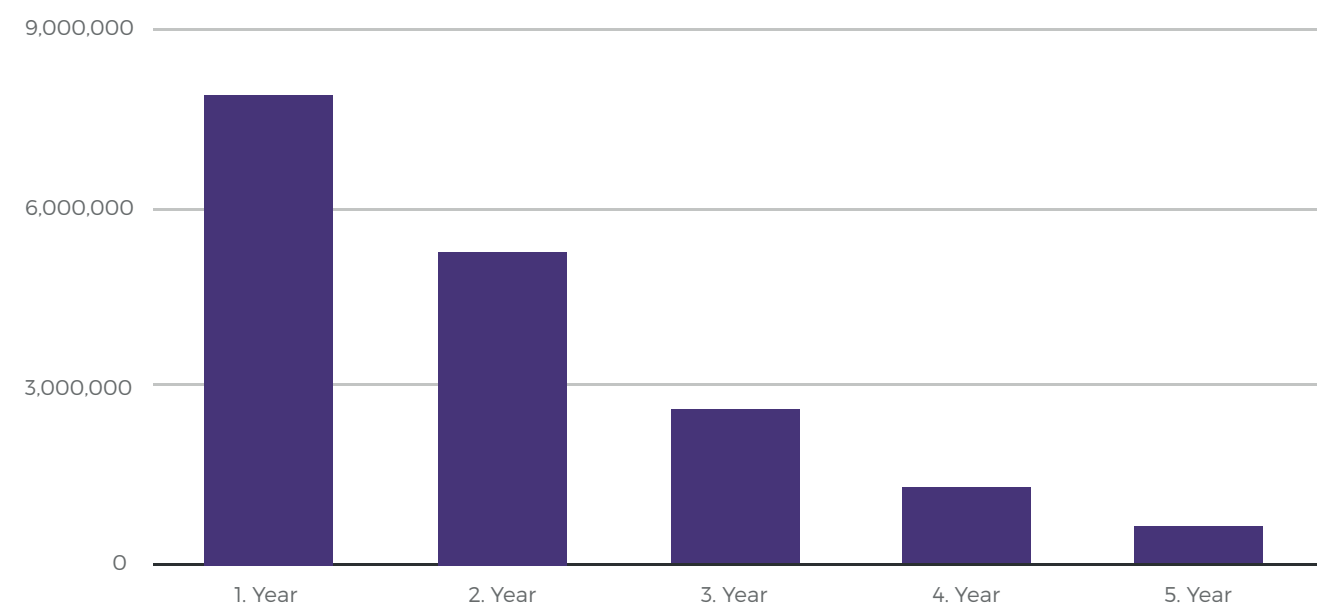
Just like every concept or approach may have its own benefits and downsides, PoW has its own downside some of which are as below:

- Requires more electric power which in turn costs the miner
- High computing power hardware which is expensive
- Possibility of miners moving their hardware to mine a different coin if the reward is better there(loyalty)
- With more and more coins getting released, miner's reward would come down as the coin becomes scarce to mine

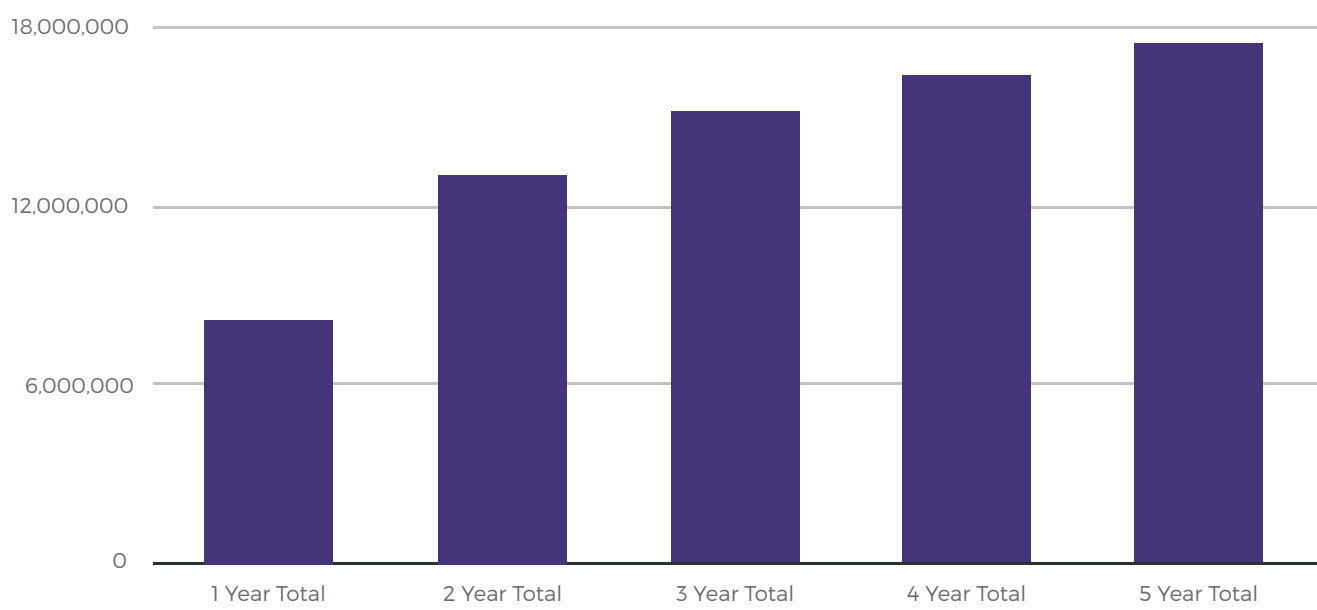
# Coin Distribution

FOLM will distribute for POW 7,884,000 FLM first year, 5,256,000 FLM second year, 2,628,000 FLM third year, 1,314,000 FLM fourth year, 657,000 FLM fifth year and 23.001.916 FLM total in 32 years.

Distributed Coins Each Year



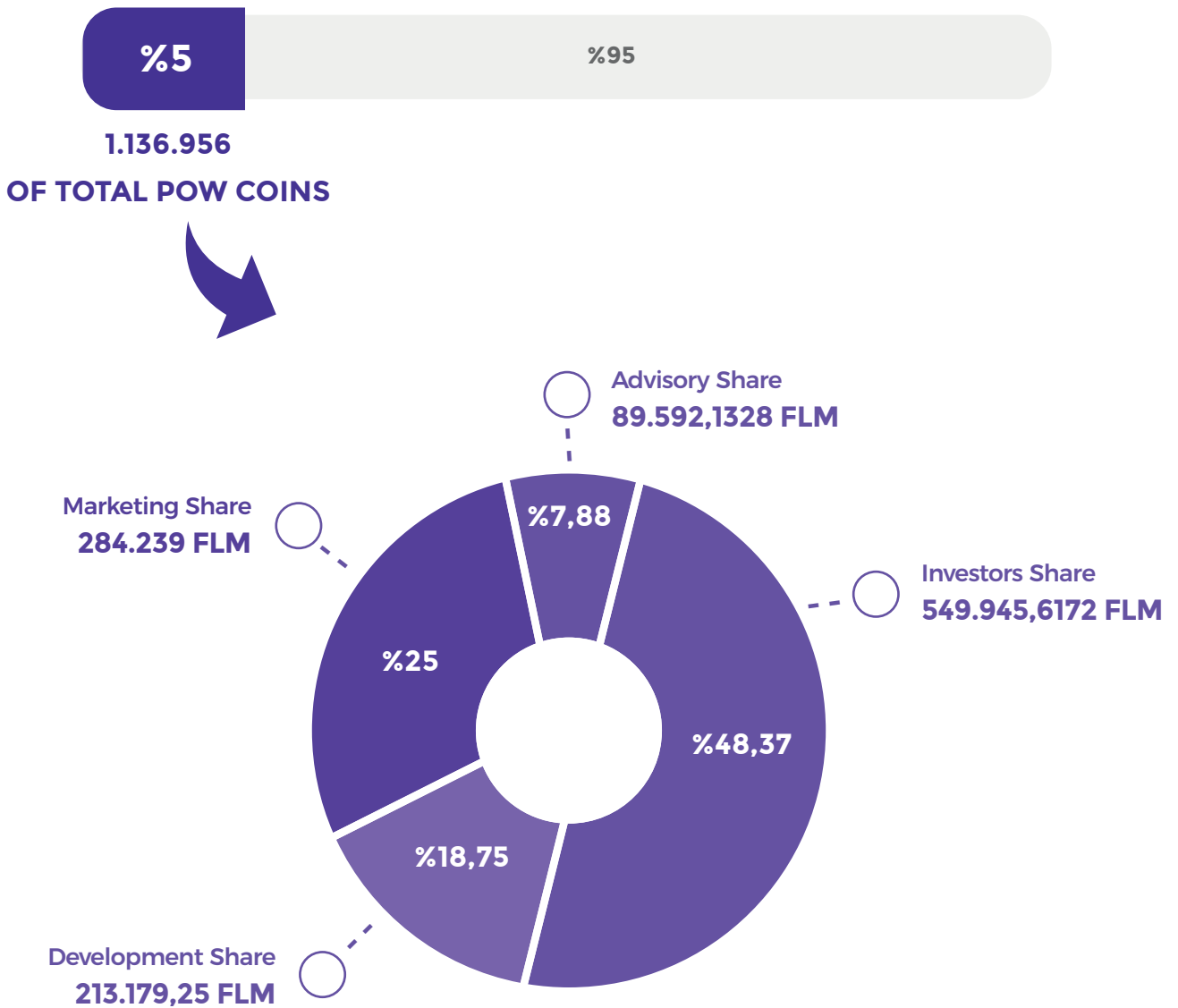
Distributed Coins Total





# Premine

Folm team have %5 of premind of POW coins to use for developing, marketing, advertising and for investors. It is less than %5 of total supply.



# Masternodes

Masternodes are, in fact, a decentralized web of computers that serve FOLM.

Masternodes perform important network functions and distribute block prizes. They help fix the coin demand, process it and serve the FOLM ecosystem.

Masternode activation requires 5000 FLM and some technical knowledge for operations. Any wallet that controls 5000 FLM can create a Masternode.

<b>1. Obfuscation / Coin Mixing</b>	19
<b>2. SwiftTX</b>	19
<b>3. Sporks</b>	19
<b>4. TOR &amp; IPV6 Masternodes</b>	19
<b>5. Community Importance and the Governance System</b>	20
<b>6. Setting up a FOLM Masternode</b>	20

# Obfuscation Coin Mixing

Folm is based on Coin join but is designed in a centralized manner through various enhancements and improvements discussed through the original coin channel. It provides a superior level of privacy during this process.

Although not incredibly anonymous, obfuscation keeps the standard bit processing threshold stable through node blending. As an example, all Bitcoin operations are transparent. For Folm, a malicious actor would need to control more than 50% of the Masternodes. It is quite high and significant enough that a single process anonymization ratio of less than 0.5% is mixed.

The 8-Round Obfuscation (Kiraly 2017b) feature is an important feature for complicating anonymous operations for FLM users.

## Sporks

The Folm network uses a multi-stage fork mechanism known as "Sporking". This feature will allow the FLM network to implement new features and open the desired network. Spork changes are deployable via the node software can be turned on and off as required by the network. For security reasons, the updates (Strophy 2017) feature is extremely useful and allows the network to react.

# SwiftTX

SwiftTX provides Masternodes with the ability to negotiate and lock transactions. When any process is sent to the network, a group of Masternodes will work to verify the operation. All Masternodes in the group are locked to join the Blockchain, if they agree on the correctness of the operation. Compared to the more common system on this side (faster by confirming more than one bitcoin during the 10 minute block timing). SwiftTX allows multiple operations to be performed at the same time, with the same location in front of a block on the top of the network. This system is based on Dash's InstantSend (Kiraly 2017a).

## TOR & IPV6 Masternodes

Folm allows the user to run the full node (or Masternode) from an onion address or an IPV6 address. FOLM will work to add full TOR nodes to both options. The unique experience of Folm users working in the TOR network itself and in the mode has been arranged for you.

The unique feature of TOR Masternode support is as a secret service to run your Masternode.

Tor nodes also provide users with stable internet connectivity.

Masternodes solve the aggression and reconciliation problems by removing the confidentialities from their home networks without affecting them, thereby removing the threats posed by location or home networking exploits.

# Community Importance and the Governance System

The most important factor behind long-term success is expected to be the Folm community. Also important is the ability to influence the future of the coin in a meaningful way. For this reason, we think that the POW process over the network will eventually activate the budgeted superblocks.

These superblocks, paid at a monthly rate, will enable the community to significantly control the development of Folm over all aspects including its brand presence. Delaying the activation of this system will save us time. We have also made available some block rewards so that miners and Masternode owners overall have a great positive user experience.

# Setting up a FOLM Masternode

FOLM requests that exactly 5000 FLM be sent to any FOLM wallet address in a single transaction. There should not be more or less, otherwise it will not work.

It is similar to the working principle of other Masternodes cryptocurrencies.

You can also setup multiple Masternodes (of course, multiple IPs are required). Also important is the fact that we must ensure that each address exactly holds 5,000 FLM to start a masternode and requires at least 15 confirmations. After the Masternode has started, you can of course move the gained coins over 5000 FLM to another wallet.

For more detail please check this link :  
<https://folm.io/blog/masternode-setup>



# Mining and Pools

FOLM uses the miner friendly crypto algorithm (PHI1612) which consumes less energy. Also FOLM is an ASIC and Nicehash resistant coin.

You can see our mining statics for this link  
<https://explorer.folm.io>

You can see actual pool list for this link  
<https://folm.io/pool-list>

Pool	Fee	Location	Worker	Hashrate	24h Block	Last Block
Kwchmining.com	0.5 %	US	916	55.62 Gh/s	332	16129
Coin-Miners.info	1 %	EU	4756	38.24 Gh/s	172	16130
Bsod.pw	0.9 %	EU	131	12.34 Gh/s	80	16125
crazypool.ca	1 %	EU-US	16	1.76 Gh/s	3	16084
zergpool.com	0 %	EU-US	337	1.60 Gh/s	54	16115
corpopool.com	0.5 %	EU	8	1.28 Gh/s	12	16123
Protopool.net	1 %	EU	17	689.64 Mh/s	9	16104
blockmunch.club	0.25 %	US	15	618.42 Mh/s	5	16119
leech.skunz.ru	0.1 %	EU	6	243.53 Mh/s	3	0
fairmine.pro	1 %	EU	2	240.25 Mh/s	1	0
Poolr.io	0.4 %	US	2	63.68 Mh/s	1	15730
xaiten.com	0.9 %	AS	0	0.00 h/s 0	11734	
MiningPool.shop	0.9 %	EU-AS	0	0.00 h/s 0	7854	
Masterhash.us	0.5 %	EU-AU	0	0.00 h/s 0	33	
saltpool.net	0 %	US	0	0.00 h/s 0	4088	
Doufen.com	1 %	EU	0	0.00 h/s 0	0	
Total			6206	101.22 Gh/s *	683*	16130*

\* This is the state of the network at the time of writing



# Road Map For 2018-2019



## Q1 2018

- ✓ Coin launch 17 FEB
- ✓ Listing at pools
- ✓ Exchanges listing
- ✓ Whitepaper
- ✓ Masternode profit websites listing
- ✓ Bounty Campaigns
- ✓ Mac OS wallet
- CoinMarketCap listing

## Q2 2018

- More exchanges listing
- WhatToMine listing
- Web Wallet
- Android wallet
- iOS wallet
- Official Announcement of Folmbank
- Business Whitepaper

## Q3 2018

- Well-known third-party wallets integration
- Codebase upgrade
- Atomic swaps implementation
- Launching FolmBank (Beta)**
- Meetinging the Team

## Q4 2018 - 2019

- New wallet with trading integration
- Trading direct trade function FLM/BTC
- Releasing new Roadmap

# Downloads & Useful Links



Block Explorer



Windows



Linux



Paper Wallet



Github



Paper Online



Nvidia Miner



Amd Miner

## Community



Discord



BitcoinTalk



Telegram



Twitter



Instagram



Facebook



Twitch



Reddit

# Join Us !

**WE ♥  
FOLM**

simple  
innovative  
and cutting-edge  
cryptocurrency





**FOLMCOIN**

# **BACK to the FUTURE**

Folm will be the cryptocurrency of tomorrow



**FOLMCOIN**

[www.folm.io](http://www.folm.io)

# References

DASH Masternodes	<a href="https://dashpay.atlassian.net/wiki/display/DOC/Masternodes">https://dashpay.atlassian.net/wiki/display/DOC/Masternodes</a>
DASH InstantSend	<a href="https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend">https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend</a>
DASH PrivateSend	<a href="https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend">https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend</a>
Bulwark Whitepaper	<a href="https://bulwarkcrypto.com/docs/EN_-_Bulwark_Cryptocurrency_Whitepaper.pdf">https://bulwarkcrypto.com/docs/EN_-_Bulwark_Cryptocurrency_Whitepaper.pdf</a>
PIVX Whitepaper	<a href="https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-TechnincaI-Notes.pdf">https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-TechnincaI-Notes.pdf</a>
LUX Whitepaper	<a href="https://www.luxcore.io/LUX_WP_V1_NOV_2017.pdf">https://www.luxcore.io/LUX_WP_V1_NOV_2017.pdf</a>
Bitcoin Developer	<a href="https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf">https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf</a>
Cubehash	<a href="https://eprint.iacr.org/2009/342.pdf">https://eprint.iacr.org/2009/342.pdf</a>
Fugue	<a href="https://eprint.iacr.org/2014/423.pdf">https://eprint.iacr.org/2014/423.pdf</a>
Gost	<a href="https://www.esat.kuleuven.be/cosic/publications/article-2091.pdf">https://www.esat.kuleuven.be/cosic/publications/article-2091.pdf</a>
Echo	<a href="https://eprint.iacr.org/2010/364.pdf">https://eprint.iacr.org/2010/364.pdf</a>
Skein	<a href="http://www.skein-hash.info/sites/default/files/skein1.3.pdf">http://www.skein-hash.info/sites/default/files/skein1.3.pdf</a>
Jh	<a href="http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf">http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf</a>