Vlad Cristian
Bucharest, Romania

April, 2017

MaskNetwork

A p2p decentralized social trading network

Introduction

MaskNetwork is a social trading network that **rewards** bloggers and traders for their effort in creating content. The network allows users to trade any type of asset such as stocks, currencies, cryptocurrencies, indices, or any other asset for which a data feed is defined. Not only are users able to trade **anonymously** but certain user categories are also rewarded by the network. The process by which rewards are paid is automatically done every 24 hours, without external or third party intervention.

MaskNetwork is new software. It was written from scratch in the past two years and is not fork of an existing software. It aims to fully decentralize the retail trading area, which has grown enormously in recent years, but which is over-regulated and lacks transparency. It is and will always be **open source**.

MaskNetwork can be accessed through **web nodes**. A web node is a website that allows you to access all MaskNetwork features like sending transactions or securing addresses. A web node is the easiest method of using the network. Running a web node is a great way to spread the word about MaskNetwork and make money in the same time.

Retail trading market

There are two basic types of traders : **retail** and institutional. **Retail traders**, often referred to as individual traders, buy or sell securities for personal account. Institutional traders buy and sell securities for accounts they manage for a group or institution. Pension funds, mutual fund families, insurance companies and exchange traded funds (ETFs) are common institutional traders.

Prior to the development of online trading platforms in the late 90s, trading was restricted to large financial institutions. It was the development of the internet, trading software, and forex brokers allowing trading on margin that started the growth of retail trading. In the last years, traders were able to trade spot currencies or stocks with market makers on margin. This mean they needed to put down only a small percentage of the trade size and can buy and sell currencies in seconds.

Retail online trading has been promoted by some as an easy way to make profits. As a result, the number of individual traders and brokers increased steadily as did trading volumes.

At present there are hundreds of active brokers on the market while new brokers and new traders are entering the market every month. Many of the new traders do not have any trading experience and are attracted to misleading advertisements promising quick profits with minimal effort. They don't understand how damaging a large spread is for their future profits or how easy they can be manipulated by brokers.
Conforming to BIS (Bank for International Settlements), in 2013

- Retail traders where predominantly male
- Madian age is 35
- There where **4 millions** traders spread around the globe
- 1.4 million live in **Europe**
- 1.6 million live in **Asia**
- Only 150.000 live in US

Why MaskNetwork ?

In all investments, there is a risk of **investment fraud**. This risk can increase for online brokers where the investor does not have a personal relationship and the broker may be located in a different jurisdiction. As we have mentioned before, retail online trading has been promoted by some as an easy way to make profits and has thus been the focus for a number of **frauds**. In response, financial regulators in a number of countries have introduced **permanent restrictions** and provided warnings about this type of trading as well as legal actions against perpetrators.

As a result of regulatory framework and associated costs, brokers imposed higher **minimum** fees / transaction sizes while all of them **forced** traders to provide identification data like Photo IDs, proof of residence and so on.

These are the main problems faced by the retail trading market

- Lack of **transparency** of brokers. You can sell and buy hundreds of times the EURUSD pair without knowing what's going on behind or how financially stable your broker is. Brokers are still **black boxes** for end users.
- **High fee**s (especially for trading shares)
- Minimum transaction sizes
- Maximum leverages imposed by regulators

- AML, KNY rules **imposed** on all traders
- Huge entry costs for new brokers.
- Inability of most European / Asian brokers to serve US customers (due to regulation).

In the end regulation solved nothing. Retail trading market is not transparent, it has high entry costs and in the last years became over-regulated. **We believe the retail trading market is the perfect candidate to be disrupted and decentralized.** And we think we have a solution.

MaskCoin

MaskCoin (MSK) is the cryptographic currency underlying the network. For any service or transaction, users will pay a small fee in MaskCoin. The number of coins is limited to **21,000,000** which will be slowly distributed to miners and content creators.

Default Network Address

Unlike other networks like Bitcoin, where a small amount of coins is created every day, in MaskNetwork all coins are created on the first block and stored in a special address called **Default Network Address (DNA)**. This address does not have a private key and is entirely controlled by the software. Default Network Address receives all user-paid fees and distributes rewards to miners and creators every day.

Network Fees

As mentioned for any transaction / service, users will pay a fee. Fees are essential to avoid spam attacks. Fees vary depending on the service used. Unlike other systems, in MaskNetwork, fees **do not go to miners** but go to Default Network Address. Miners will always be paid by network, not by users. Below are some examples of fees

- Sending coins to another address - 0.1% of amount sent
- Sending assets to another address - 0.0001 MSK for every unit of asset sent

- Renting a name for your address - 0.0001 MSK / day
- Restricting recipients - 0.0001 MSK / day

On top of this, all addresses will pay a fee of 0.0001 MSK / day (~1440 blocks). Empty addresses will be removed from the distributed ledger and will be reincluded when they receive funds. This fee is essential to get rid of inactive addresses holding very small quantities of MSK. As a general rule any MaskNetwork address will pay 0.0365 MSK / year as a maintenance fee.

Distribution

Every year, the network uses **5% of undistributed** coins to reward miners and content creators. This means **~ 0.013% / day** of the undistributed amount. The maximum annual inflation rate is 5%. Because in the first years the undistributed quantity will decrease every day, the rewards pool will be smaller and smaller each day.

For example, block reward decreases 0.0001 MSK every two blocks. Undistributed coins are held by Default Network Address. This address' balance will never reach 0 MSK because it will distribute fewer and fewer coins. Sooner or later, the earnings of this address (from the fees) will be higher than the rewards paid to users. There are 3 scenarios:

- The default address spends more coins that receives from fees - rewards decrease each day
-
- The default address receives the same amount of coins it spends - the rewards tend to remain unchanged

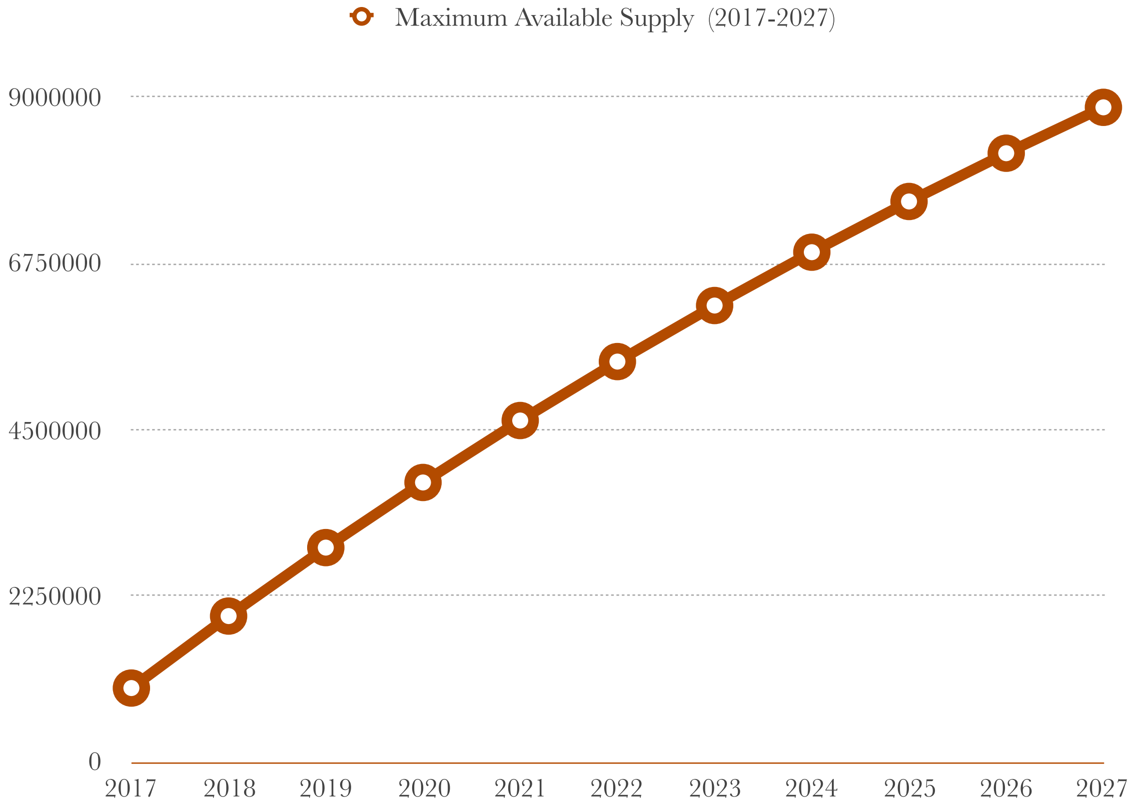
- The default address receives from fees more than it spends on rewards - rewards tend to increase every day

In the long run, the revenue / spending of Default Network Address ratio will tend to 1.

Initially, the default network address will hold 20.000.000 coins (1.000.000 reserved for ICO, bounties and the developers). In the first year, a maximum of 975.477 coins will be distributed. This quantity will gradually decrease, and in

2027 only 621.972 coins will be distributed. This is the extreme case where the default address has no revenue. Depending on the revenue received, the amounts distributed will be slightly higher. But never more than 5% of the default network address balance will be distributed per year.

Below is a chart showing the **maximum available supply** of coins in the next 10 years (in case the default network address has no income which is impossible). In case fees amount become really high due to increased adoption the total supply will tend to remain unchanged from year to year.



Premine and the ICO

At block 0, **635.000** coins (**3%** of total number of coins) will be deposited in ICO participants addresses / bounty participants / developers address. ICO will be launched in June, 2017. The funds received will help the team develop the project and MaskNetwork ecosystem in the following years. Our target is to sell 500.000 coins during ICO. **All unsold coins will be deposited in developer's address.** Also 10.000 coins will be used for bounties. Another 25.000 coins were distributed during the pre-sale held back in 2016. Developers will receive 100.000 coins plus any unsold coins during ICO.

Rewards distribution

There are two main categories of rewarded network users. The first category is the miners that maintain network security (MaskNetwork uses an innovative POW algorithm) and the second category is represented by content creators such as bloggers, data feeds providers, asset issuers, and so on. Check below for a detailed chart of distribution.

Miners are rewarded after each block created. The rest of the users are rewarded every 1440 blocks (~ 24 hours). Payment of rewards is hard-coded in the network code and is done automatically based on clear rules without any outside intervention.

As mentioned above, multiple categories of users are rewarded. Except for miners that are rewarded each block, the content is rewarded based on the votes received from users.

Votes

Voters are heavily rewarded for curation. Voters usually receives 50% of content reward. For example if a blog post receives 10 MSK in rewards, 5 MSK goes to content owner and 5 MSK is distributed to voters (curators) that uprooted / down voted the content.

Any address that holds at least 0.1 MSK can upvote or downvote content. The power of voting is based on the MSK balance of the voted address and the time of voting. After each vote, the address voting power decreases. The voting power of the address is calculated by the formula

$$\mathbf{P = B / N}$$

P = voting power
B = address balance in MSK and
N = the number of votes in the last 24 hours.

In case of Blog posts, comments or binary options the vote power decreases 0.07% / block from the time content is posted.

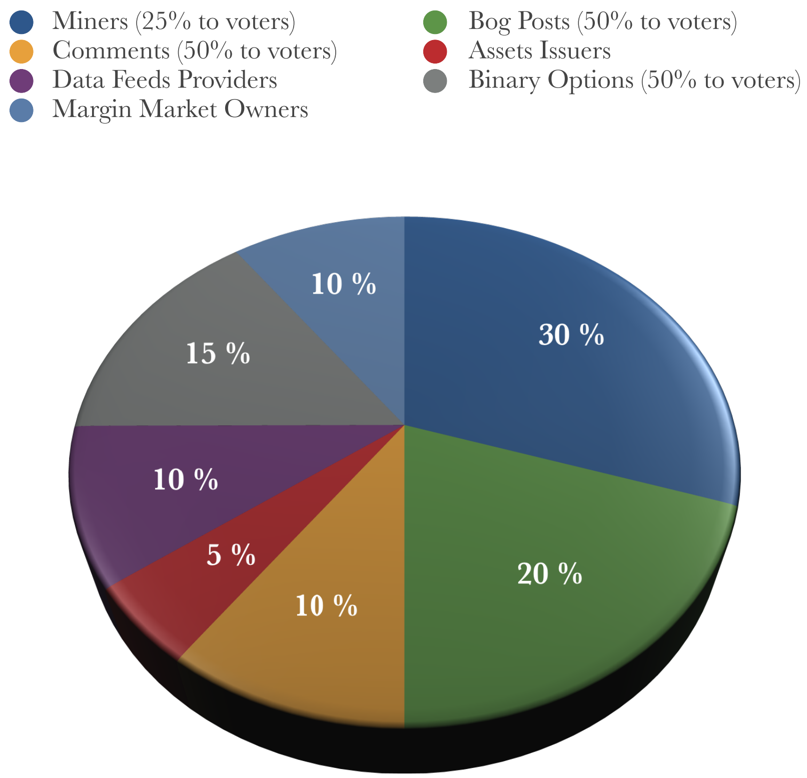
$$P = P-(0.07 * T * P/100)$$

P = voting power
T = number of blocks since the content was first created

Below is an example :

A blog post is posted at block **1000**. An address holding 10 MSK that has no votes in the last 24 hours up vote the content 10 blocks after posting (~ 10 minutes after posting). The vote power is **9.93 points**. The same blog post is voted at block **2000** (~16 hours after posting) by an address holding **500 coins** that already voted **4 other** blog posts. The vote power will be only **30 points**. Even if the address has a balance x50 bigger than the initial vote, **the time of voting and the previous number of votes** decreased the address voting power.

Each category of content creators / miners have it's own reward pool. Below is a chart presenting rewards distribution by user type. Keep in mind that the **daily reward pool is 0.013%** of Default Network Address. Because this balance will decrease in the first years, the reward pool will be **smaller** and smaller every single day.



When and how content creators / miners are rewarded

Miners are rewarded after each block created. Miners' block reward drops with ~ 0.00000001 MSK on every two blocks mined. Miners will pay **25% of the reward to voters**. In MaskNetwork users can up vote / down vote miners. Depending on the votes received, miners will work on a higher / lower difficulty. Unlike other systems, in MaskNetwork, not all miners are working on the same difficulty. If they are heavily down voted by stakeholders it will be more difficult for them to mine new blocks. without equipment upgrades / more cash spent on electricity. Miner's reward pool is **30%** of total reward pool.

Bloggers are rewarded every 1440 blocks (~ 24 hours) depending on the votes they receive. The reward is shared with those who voted the post. **Only 50%** of the prize will go to the person who created the post. Bloggers reward pool is **20%** of total reward pool

Commentators also have a separate reward pool. Users can comment on blog posts or other categories of content and can be up voted or down voted. Like bloggers, they will receive 50% of the prize. The other half goes to voters. Commentators reward pool is **10%** of total reward pool.

Asset issuers will receive 5% of total reward pool. They will not split this reward with voters. Users can't directly up vote an asset. The asset will be automatically be up voted by an address when the address receives an asset. Assets can't be down voted.

Data feed providers receive 10% of total daily reward pool. **Data feed** is a mechanism for MaskNetwork users to receive updated **data** from **data** sources. Based on data feeds, binary options or margin markets can be launched. When a user buys a binary option or trade on a market based on a data feed, that data feed gets an up vote from that address. This is how data feeds are rewarded. Data feed owners don't split the reward with voters.

Binary options issuers receive **15%** of daily reward pool. Rewards are distributed every 1440 blocks. Like bloggers, option issuers will receive only **50%** of the reward. The other half goes to voters.

Margin markets operators will receive **10%** of daily reward pool. Over MaskNetwork, margin markets allow users to trade on margin a specific asset. Like binary options, margin markets are based on data feeds. In the real world buying on margin is borrowing money from a broker to purchase stock. You can think of it as a loan from your brokerage. Over MaskNetwork, a margin market allows you to place leveraged bets against the market owner. Margin markets prices are provided by data feeds. All your losses are market owner's gains and vice versa. Not only that traders don't pay any interest but margin market operators are rewarded by network every 24 hours for their effort and risk. Margin markets operators don't split the reward with voters. You can't directly up vote a margin market. The market will automatically be up voted when a user place a leveraged position.

Basic network features

The network has two features layers. The first deals with basic operations like transactions, addresses, messaging and so on. The second implements the trading modules like data feeds, binary options or margin markets.

Addresses

A **MaskNetwork address**, or simply **address**, is an identifier of **108-212** alphanumeric characters, that represents a possible destination for a MaskCoin or asset payment. Addresses can be generated at no cost by any user of MaskNetwork using any web wallet. It is also possible to get a MaskCoin address using an account at an exchange.

The most important aspect of MaskNetwork addresses is that an address is actually the **concatenation, in Base58 format, of the public key**. That means you can send **encrypted messages / data to any address** with **no additional info** required even if the address was never used before. The built in messaging system provides exactly this function of sending secure, encrypted messages between addresses. See details below.

Creating addresses can be done without an Internet connection and does not require any contact or registration with the MaskCoin network. It is possible to create large batches of addresses offline using freely available software tools like the official paper wallet generator. Generating batches of addresses is useful in several scenarios, such as e-commerce websites where a unique pre-generated address is dispensed to each customer who chooses a "pay with MaskCoin" option.

MaskNetwork addresses are case-sensitiveand should be copied and pasted using the computer's clipboard wherever possible. If you hand-key a MaskNetwork address, and each character is not transcribed exactly - including capitalization the funds could never be recovered.

This is the reason the network provides and alias system, that allows users to rent an **address name** like marry or casino and those who want to send others funds can use this alias. Manually typing a raw network address is not recommended.

Address Names (Aliases)

The Alias System is one of MaskNetwork simplest but most powerful features. MaskNetwork Alias System essentially allows you to associate a name (up to 2-30 alphanumeric characters) to an address. This means that a long, complicated or impossible-to-remember string of data like a network raw address ID can be replaced by a shorter one.

The main advantage of this is the convenience it offers. You can use a single word to represent something far more complex: your address details. Users can rent an address name for 0.0001 MSK / day using any wallet in 3 clicks. The fee is sent to default network address and is one of the network income streams.

Aliases can be rented on any period starting from 10 days. The alias will be automatically removed from the distributed ledger when the expiration block is mined. They behave just like internet domain names.

Aliases can be transferred to other addresses. Users can transfer them using any web wallet. The costs are only 0.0001 MSK / transfer. This option makes it easy to trade names with users who do not want to use the built-in address market.

The network also provides users with a decentralised p2p marketplace where address names can be traded in a safe and risk-free. Users who want to sell an address name can easily do it using any web wallet. The price is expressed in MSK. Once a price is set, the offer for sale will be listed and potential buyers can acquire the name in 2-3 clicks. Funds are transferred by the network from the buyer to the former owner without any external intervention to escrower.

MaskNetwork address names market is the perfect example of a decentralized p2p market where nobody knows anybody, but everyone can trade with zero risks.

Address Profiles

Users who want to provide more information about themselves or their company have the possibility to set up a public profile. Address profiles are exactly like facebook profiles. Users can provide contact information, a brief description, a profile picture or other details.

Because these profiles are retained in the block chain, they are public by default. The profile setting fee is 0.0001 MSK / day. An address can have only one active profile.

Restricted recipients

Restricting recipients is one of the best ways to protect your funds. If this feature is enabled, an address can only send funds to a maximum of 3 other predefined addresses. Any other transfer will be declined by the network.

Restricting recipients can be done easily, using any web nodes. Once enabled, the option can no longer be canceled. By linking these options to multiple addresses, it is possible to create highly complex multi signature schemes. Those are especially useful if used by companies or other organisations.

For example, address A could be set to send funds only to B and C addresses, and B and C addresses only to D.

Enable this option is perfect in case the user operates on a public web node where the operator has access to all private keys. Even if the owner of the node owns the private key, it can only move funds to up to three addresses that also belong to the address owner. In this way, the address owner can continue to work (votes, writing articles, etc.) without the risk of losing their funds.

Transactions

A **transaction** is a transfer of MaskCoin / asset value that is broadcast to the network and collected into blocks just like any other packet type. A transaction moves funds or assets from an address to another.

Transactions may have only **one** source and one destination. Transactions with multiple sources / recipients are not supported. Transactions are not encrypted, so it is possible to browse and view every transaction ever collected into a block.

All transactions are **visible** in the block chain. Any web wallet includes a block chain browser where every transaction included within the block chain can be viewed in human-readable terms. This is useful for seeing the technical details of transactions in action and for verifying payments.

If the transaction is denominated in MSK, the sender will pay a fee of **0.1%** the transacted value. The fee goes to the default network address and is the **main revenue source** of the network. Transactions can also move assets between addresses. If the transaction transfers an asset, then the fee will be **0.0001 MSK / asset** transferred. The fee will also be paid by sender.

Asset issuers can specify a **transfer fee and an address** where this transfer fee will be received. This transfer fee will be paid by the recipient of an asset transaction. The fee is denominated in that asset and will be sent to the address indicated by the asset issuer and **not** to the default network address. As a general rule, default network address can **only receive MSK.** In case no transfer fees are specified by issuer, the recipient will not pay anything.

In order to be able to receive an asset, users have to '**trust**' an asset first. Trusting an asset is an easy process that can be made using a web wallet. Once an asset is trusted, the user is able to **receive** transactions denominated in that asset.

Every time a user receives an asset transactions the recipient address **will up vote** the asset. Up votes are reset every **24 hours**. Only one vote / asset / 24 hours is allowed. Based on those up votes the asset issuer will be **rewarded** at the end of the day.

Messages can be attached to any MaskNetwork transaction, making bookkeeping easy, as you can tag all your transactions with a description. Project developers can use the Messaging system to embed machine-readable data within an MaskNetwork transaction. This allows automated functions by reading the data sent to you on the blockchain. All messages are securely encrypted and only the receiver can decrypt it.

Escrow Transactions

Users can also send **escrowed transactions** where a trusted third party securely holds buyer's coins in escrow until the terms of the sale are met and as a result the buyer or the escrow address release payment to the seller. Escrow transactions are built-in the MaskNetwork protocol.

Sending an escrow transaction is a trivial process especially if all the parties involved use a web wallet. All the sender has to do to initiate an escrow transaction is to specify an escrow address. If such an address is specified, the funds will leave the sender but will not reach the recipient.

The escrow address does not own the funds so the risk of fraud is completely eliminated. Funds are blocked by the network for a maximum of one month, until one party makes a decision.

- The sender can only **release** the funds to the recipient.
- The recipient may only **remit** the sender's funds back.
- The escrow address can **release** the funds to the recipient or **remit** the funds back to the sender.

An escrow transaction costs **0.0030 MSK** more than a regular one. When an escrow transaction is initiated, all parties are informed and can make a decision within 30 days. Decision means a signed package that once included in a block will release the funds.

Messaging

The MaskNetwork Messaging system allows you to send and receive data on the MaskNetwork Blockchain, thus allowing any network address holder to communicate directly with any other addresses.All messages are securely encrypted and only the receiver can decrypt it even if it traverse the whole network. Because a MaskNetwork address is a Base64 coded public key, the sender doesn't need additional info in order to send a message to an address even if that address was never used before.

Sending a message can be done easily using any web wallet. Messages are delivered instantly even if they were not included in a block. This makes it possible in the future to create p2p encrypted instant messaging applications.

Sending a message cost 0.0001 MSK.

Blogs and comments

A blog is a frequently updated online personal journal or diary. It is a place to express yourself to the world. A place to share your thoughts and your passions. Really, it's anything you want it to be. For our purposes we'll say that a blog is your own website that you are going to update on an ongoing basis. Blog is a short form for the word weblog and the two words are used interchangeably.

MaskNetwork allows users to create and manage their own anonymous blog. If other users feel that a post is original and informative they can up vote it. Depending on the number / strength of votes received every 24 hours, bloggers are rewarded in MaskCoins.

20% of total daily reward pool is reserved for bloggers and voters. The reward is shared with those who voted the post. Only 50% of the reward will be received by blogger. The rest will be distributed to voters.

Users can also down vote a blog post. The total votes power a blog posts receives is calculated using the formula

$$\mathbf{TVP=UP-DP}$$

VP = votes power
UP = up votes power
DP = down votes power

The blog post will be rewarded depending on the total votes power received. Both up voters and down voters are rewarded even if the down voters can significantly reduce the reward amount.

Users can vote a blog post once every 1440 blocks. A blog post can be voted multiple times by the same address while it's online and visible and they can be rewarded many days after initial publishing in case they receive enough votes.

Users can maintain their blog using the tools provided by web wallets. Posting a blog post cost 0.0001 MSK / day. Users can publish a post blog for at least 30 days but may extend this period if they so wish. After this period expires, the post is removed from the distributed ledger and can't be voted anymore.

Users can also comment on a post. Just like blog posts, comments can be up voted / down voted and the authors rewarded. Commentators have their own reward pool. Every 1440 blocks (~24 hours) 10% of total daily reward pool is used to reward comments. Commentators will split this reward with voters just like bloggers do.

Follow / Unfollow

Following someone means you've chosen to subscribe to their MaskNetwork updates. When you follow an address, every time they post a new blog post, it will appear on your home timeline. Following an address costs 0.0001 MSK / day. You can follow an unlimited number of addresses. If you think an address's post has become worthless, you can unfollow that address by paying a fee of 0.0001 MSK.

Just like any other action, following / unfollowing an address can be made using a web wallet.

Advanced network features

Data feeds

Data feed is a mechanism for MaskNetwork users to receive updated **data** from **data** sources. Data feeds could present the last price of a stock or the last temperature recorder in London. There is no limit on what data feeds can represent.

Any user can setup a new data feed. All they need is a reliable **data source** (a web page for example) that will provide the data in a predefined format (read the data feeds technical documentation for more info).

A data feed consists of several **branches**. Each branch presents the price of a **single** external asset. For example, if you want to present the EURUSD price and the GBPUSD price of the network, you will need to create a two-branch data stream. A data stream can contain up to **1,000 branche**s. Setting a branch costs **0.0001 MSK / day.**

Once setup the wallet will query the data source every minute, grab the data, format and broadcast the feed packet. Once included in a block, the nodes will **update** the last prices accordingly. This process is **fully automated** with no user intervention. All you need to do is make sure the data source (web page) is up to date and accessible over the web. The web wallet software will do the rest.

Based on votes received, data feeds are also **rewarded** by the network. The most important difference from blog posts is that a data feed **can not** be **manually** up voted / down voted. A data feed is up voted automatically when a user buys a binary option or launch a transaction using a market that uses the data stream. Also, data feeds operators do not share the rewards with voters.

Based on data feeds, binary options or margin markets can be launched. Suppose an address (A) launches a binary option using a data feed (D). When an address (B) will buy the binary option, it will **automatically** up vote the data feed (D) used by the operator. Also, address A will up vote the data stream (D). Data feeds can not be down voted.

Data feeds have their own reward pool consisting in **10%** of total daily reward pool and are rewarded every 1440 blocks (~24 hours).

User Issued Assets (UIA)

An asset is a digital token that can be transferred between addresses in the same way that MaskCoins are transferred. The main difference between an user issued asset and MaskCoin is that an asset is **issued** by a user and not by the network as a whole.

MaskNetwork assets are a convenient way to represent anything fungible and tradeable. An asset token could represent a bar of silver, a pizza redemption coupon, a share in a company, even a portion of a portfolio of other assets. By representing these things digitally on the blockchain, they can be publicly verified and easily traded.

The MaskNetwork assets are based on the concept of the 'colored coin'. More specifically, MaskNetwork assets are based on the ability of the blockchain to recognise and therefore trace the origin of transactions involving a coin or a set of coins which have been designated to represent any type of asset you can imagine, whether digital (for example, stocks, bonds, smart property) or tangible (for example, cars, houses, precious metals etc).

An asset is under the full **control** of the person who created it. Those who issue assets can **increase** the available supply whenever they want. Assets issued by users do not have a limited amount. Once the asset is issued, the whole qty belongs to the creator.

The value of an asset depends on issuer. For example, if someone issues an asset representing 1 gram of virtual gold that can be bought or sold for 1 gr of real gold, its value depends exclusively on the the person who issued it. If the issuer disappears, or refuses to give you one gr. of real gold for 1 asset, the value of that asset will become zero in no time.

Any user can issue his / her own asset. Issuing an asset can be done very easily using a web wallet. The creator has to provide a few details such as asset name, symbol, brief description and eventually a transfer fee.

The issuer may charge a transfer fee that will be paid by the beneficiary of an asset transaction. The fee will be denominated in the asset and represents a maximum of 5% of the amount received. The fee is sent to an address specified by the issuer. For example if the transfer fee of asset TESTTE is 1%, and a user receives 10 TESTTE, he / she will pay a fee of 0.1 TESTTE. The fee will be transferred to an address owned by the issuer.

Assets issuers are also rewarded by the network. Each time a user sends assets to another address, the asset will automatically be up voted by the sender. Based on these votes, every 1440 blocks assets issuers will be rewarded by the network.

Assets have their own reward pool consisting of 5% of the daily reward pool. Assets as well as data feeds can not be voted manually and can not be down voted.

Assets can also be used as currency in binary options or margin markets if the binary option or market has been set to use that asset.

An asset is identified by its symbol. The asset symbol is a 6-character string that uniquely identifies an asset.

Like the other categories of content, assets are issued for a limited period that can be extended. When this period expire the asset will be liquidated by network. All asset balances will be deleted. The person who issues an asset will have to pay a fee that is determined using the formula

$$\mathbf{F = Q * 0.0001}$$

F = fee
Q = Initial asset qty

Another difference from MaskCoins is that an asset can not be sent to an address if the address does not **trust** the asset. We have introduced this rule to limit spam. In order for an address to be able to receive an asset, the address must first **trust** that asset. It is a simple process that can be done from the asset presentation page.

Assets Exchange

The MaskNetwork Assets Exchange is a peer-to-peer exchange built directly into the MaskNetwork software, allowing secure and fast decentralized trading in MaskNetwork Assets. This eliminates the need to transfer assets or to put trust in an outside agency or business, and as MaskNetwork Assets can be used to represent literally anything (from Bitcoin to coffee beans) there are a wide range of potential investments or trades to be made on the Asset Exchange.

The MaskNetwork Asset Exchange matches asset buyers and sellers, it works in a similar way to cryptocurrency exchanges. All asset exchange operations can be accessed using a web wallet.

Any user can launch an asset exchange. An exchange is used to buy / sell an asset for a currency. The currency may be MSK or another asset. Once launched, users can start trading. Markets allow placing buy / sell orders as well as a mechanism by which buy orders are matched with sales orders. Trading on such a market does not involve fees, except for the transaction fees paid to the asset issuer.

Because an asset exchange can be use to trade any asset for any other asset, exchanges have to be manually created by users. Those exchanges are not automatically created when an asset is issued. The fees for starting a new exchange is 0.0001 MSK / day. Also, those who place buy / sell orders will pay a MSK 0.0001 fee for their pending orders.

Binary Options

In the real world a **binary option** is a financial **option** in which the payoff is either some fixed monetary amount or nothing at all. Writing binary options is usually reserved for big traders / institutions.

MaskNetwork enables **anyone to write their own**, individual options. The trader can not only choose the direction but also assign a payout and other conditions. The created option is then broadcasted to the network. Traders can buy entire option, or just a portion, which means better risk management for every trader.

A binary option can be up voted manually but will also be automatically up voted when a user buys a portion / the whole option. Binary option issuers will split their reward with those who uprooted the option. A binary option can be manually down voted.

You can look at binary options as a **p2p bet** where the initiator publishes the conditions and provides a collateral from which buyers will be paid. The collateral is **blocked** by the network, and the initiator no longer has access to funds as long as the option is active.

Binary options are **based** on data feeds. If the price presented by the feed **meets** the conditions imposed by the option, then the network closes the option and pays the winners. Absolutely the entire process is managed by the network and all the data is public. The risks for both the initiator and the buyer of an option are **zero**.

To better understand how a binary option takes place, we'll describe the entire process below. Suppose a user wants to launch an option that sounds like this:

"All those who buy this option will earn 100% of their investment if the BTC / USD price reaches $ 2000 in the next 10 days. I agree to accept buyers for 2 days."

1. First, the one who wants to launch an option chooses a reliable data feed that provides the BTC / USD price.

2. Any wallet web allows users to launch a binary option. The user will set a name, a small description, specify the **data feed** on which the option is based,

indicate **how long** users can buy the option, and clearly set out the **conditions** in which buyers win the option. It also specify how much buyers will earn and set the **collateral size**. If he is right he will win **all the amounts** deposited by the buyers. If he loses, he will pay the buyers the invested sums **plus** the promised **bonus,** in our case 100% of buyer's investments.

3. Once **included** in a block, the option becomes **active**. The network will **block** the funds set as collateral. The option initiator has no control over the option or the funds. Everything is in control of the network.

4. Those who want to buy the option can use any web wallet. If they think they can win they can buy a **piece** or the **whole** option. In case a user decides to buy, he/she will have to specify how much will allocate to this option. The network will **block** those funds until the option ends. When the user buys the option, his/her address will **automatically up vote** the option. Based on those votes the option issuer will be rewarded. Users can also manually up vote down vote the option. The vote power depends both on voter address's balance and time of voting as described in Blogs section.

5. Users can only buy an option **within a number of blocks** specified by initiator. After this period **expires**, the network blocks any acquisition and will check after each block if the conditions imposed by issuer are met. An option can be cleared when the price presented by the data feed falls within the conditions imposed by the option or when the expiration date is reached. In our case, the option will be **terminated** if the BTC / USD price **reaches $ 2000** or if **10 days pass** without the price **reaching** that threshold.

6. If the BTC / USD price **reaches** $ 2000, the network will use the collateral to pay **buyers**. If there are any free funds, they will be returned to the option issuer.

7. If 10 days pass and the BTC / USD price **does not reach $ 2000**, then the network will send all buyer money together with the colaterall to option issuer.

The entire process is carried out independently in conditions of maximum transparency by the network software.

Another important aspect is that binary options can be set to accept MSK or **any other asset as a currency.**

Margin Markets

Margin markets are a kind of decentralized virtual market that allows users to **trade any asset on margin**. In the real world, trading on margin means **borrowing** money from your broker to buy a stock and using your investment as collateral. Usually investors will pay **interest** for borrowed money. Over Mask Network, a margin market allows users to place **leveraged** bets against the market owner. Margin markets prices are provided by data feeds. All your **losses** are market owner's **gains** and vice versa. Not only that traders don't pay any interest but margin market operators are **rewarded** by network every 24 hours.

Any user can start his own margin market. He/she only needs an initial capital as **collateral** that will be **blocked** by the network as long as the market is active. Market owners can close a margin market anytime they want. If there are open positions, they will be automatically liquidated by the network software.

Users can use any web wallet to inits

Margin market operators are also **rewarded** by the network. When a trader initiate a position using a margin market, the address used to trade will automatically **up vote** the market. Based on those votes, margin market operators are rewarded every **1440** blocks. They **don't split** the reward with voters. Margin markets reward pool is **10%** of daily reward pool.

Consensus & Mining

Consensus

The consensus algorithm implemented by MaskNetwork is called **Variable Proof of Work (VPOW)** and is derived from the classic POW used by Bitcoin and hundreds of other clones.

A **proof of work** is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated.

Bitcoin for example uses the hashcash proof of work system.

Hashcash proofs of work are used in Bitcoin for block generation. In order for a block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block. The **difficulty** of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes. Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block.

For a block to be valid it must hash to a value less than the **current target**; this means that each block indicates that work has been done generating it.

Under Bitcoin consensus algorithm the current target is the same for all miners. Under MaskNetwork VPOW, the target is higher or lower depending on the votes a miner address received from stake holders. Basically miners can be up voted / down voted just like content is and depending on a miner popularity, the target at which the miner works is bigger / lower.

A bigger target means less work for a miner to find a solution. The target for a miner that has no votes is called **default mining target** and corresponds to the highest difficulty. To better understand how VPOW works, let's take a few examples. Let’s suppose the default mining target is 1000 (mining targets are usually much bigger numbers).

- A miner was not up voted. The has to find a nonce that after PX16 hashing generates a number less than **1000**.
- A miner was up voted by 5 addresses with a total power of 50. The miner has to find a nonce that after PX16 hashing **generates a number less than 50.000**. Basically the miner will have to work on average 50 times less in order to find a block than a miner who was not been voted at all.
- A miner was up voted by 10 addresses with a total power of 350 and down voted by 3 addresses with a total power of 100. The miner has to find a nonce that after PX16 hashing generates a **number less than 250.000**.

Any address holding at least **10 MSK** can up vote / down vote miners. A vote becomes active after ~200 blocks. Miner’s target levels are recalculated after each block. Voting a miner implies a 0.1 MSK fee. **The vote never expire** but it will be **removed** if the voter balance is less than 10 MSK.

The voting power decreases according to the number of votes given to miners by the formula :

$$\mathbf{P = B / N}$$

P = vote power
B = voter address balance in MSK
N = number of miner's votes

Both miners and those who voted for it are rewarded by the network after each block. Miners reward pool is the largest. 30% of the daily reward pool goes to the miners. Miners will share rewards with their voters. Only 75% of the reward is kept by the miner. The rest goes to the voters.

Hashing algorithm

The hash algorithm is called Polymorphic X16 (PX16) and was developed by Vlad Cristian back in 2016. The algorithm represents an improvement of the X11 algorithm implemented by Dash and other networks.

The first difference from X11 is the number of hash functions used. In PX16, 16 hash functions are used to verify POW nonce instead of 11. This is the list of used hash functions used

Blake512, BMW512, CubeHash512, ECHO512, Fugue512, Groestl512, Hamsi512, JH512, Keccak512, Luffa512, SHAvite512, SIMD512, Shaba512, Skein512, SHA256, SHA512

Another important difference is that the algorithm **changes** after each block, hence the name **polymorphic**. More specifically, in X11 the order of hash functions is the same. In PX16, the hash function is **different** depending on the previous block.

For example if the last block hash is

000012cb4ff317be3cd200329ab87625af831086431976032 38b6244f0efe175

the POW check will be made based on formula

Hamsi512 (Hamsi512 (Hamsi512 (Hamsi512 (JH512 (Keccak512 (CubeHash512 (……..(nonce))))))…)))

Basically for each hexadecimal letter / number (there are 16 in total 0, 1, 2, …..a,b,c,d,e,f) a different hash function is linked. Because block hashes are unique, the exact hashing algorithm used **changes after each block and it's also unique.**

Why Variable Proof of Work / Polymorphic X16

Variable Proof of Work / Polymorphic X16 was developed in order to overcome some significant drawbacks associated with previously used cryptocurrency mining algorithms / consensus such as SHA256 (Bitcoin) or Script (Litecoin). The biggest of these drawbacks was the fact that electronics companies had developed specialist hardware, called ASICs, for mining coins which used the SHA-256 and Scrypt mining algorithms. This had the effect of making the networks more centralized – controlled by a small group of powerful miners, whereas the original vision for cryptocurrency was for ordinary users to be able to take part in securing the network and earning rewards through mining.

By designing the PX16 algorithm to be well suited to use with general purposes CPU processors and commonly used GPU graphics cards, and by cycling through many different algorithms in a different order after each block, rather than using a single algorithm, it makes it difficult for manufacturers to develop ASICs for coins which use this algorithm. Although it is possible that ASICs will eventually be produced, PX16 coins are expected to remain ASIC-resistant for at least the short and medium term future.

The use of 16 different algorithms also increases the security of coins using this method against brute force attacks. Brute force attacks against coins, such as Bitcoin, which use other algorithms are not currently possible, but may conceivably be possible at some point in the future.

Mining centralization reducing network security, reduces the number of people with a stake in running the netwok who naturally become its advocates, and may increase the likelihood of mined coins being instantly 'dumped' as businesses need to cover costs and take profits whereas individuals may not have to.

Mining centralization is also serious problem because miners can not be held accountable by shareholders. They 51% attack the network with no shareholders consent.

The best example is Bitcoin block size debate where 100% is up to miners to change the maximum block size and fork the network. Bitcoin holders are completely ignored by miners. Under VPOW, that would not have been possible.

Under the MaskNetwork algorithm (even if we talk about a POW consensus), miners can be **drastically penalized** by shareholders. If they are down voted, the difficulty they work on will explode and the number of blocks found will be **significantly lower**. Also, the miner's revenues will be drastically **reduced**. Since miners rely on hardware-intensive hardware (such as GPUs), a negative vote on the part of shareholders may mean the **death of miner’s business** due to the cost associated with maintaining equipment / income from mining.

Variable POW combined with PX16 significantly reduces the chances of mining centralisation / miners’s influence on the network while preserving the security of a POW consensus.

Mining