MASS

MASTERNODE AND STAKING SERVICE

A ProofofStake and Masternode Smartcontract on the Ethereum platform.

Clinton McLeay, Kris Borodiansky, Dennis Klungler and Kurt Knudsen
(http://mass.cloud, @MASSToken)

Table of Contents

ABSTRACT

The goal of this white paper is to outline the process of MASS token investments. MASS tokens are an ERC20 derivative and represent a share of a pool of funds used to stake in proof-of-stake (PoS) cryptocurrencies and the creation of masternodes. Staked token holders receive a fair share of rewards paid out by PoS and masternode currencies automatically and continuously. Token holders are also able to burn their entire share of MASS for a fair share of the entire Ethereum pool, minus 10%.

After the presale and ICO phase, MASS Cloud Ltd. receives 10% of the raised Ethereum to fund development and pay for initial operating costs. Bounty programs and commitments made prior to the launch each will be given 1% of the total Ethereum and MASS. This Ethereum is then removed from the investment pool. MASS Cloud Ltd. will also receive 10% of the total MASS sold which will be locked and untradeable for 1 year and its rewards will be used to grow the pool. Rewards from unstaked MASS tokens will be placed back into the pool for additional growth. After launch, there are no additional fees or percentages taken from rewards that are paid out. Only unstaked MASS can be traded or transferred. Block rewards are based on the amount of MASS and time they have been staked since the last block reward. The total number of tokens available for sale is capped at 61 million.

INTRODUCTION

Most cryptocurrencies rely on vast amounts of computing power to find a valid solution and submit a proof-of-work claim in order to obtain the reward. Examples of such currencies include Bitcoin, Litecoin, Ethereum (currently), Dogecoin, and Namecoin. As these types of currencies become more popular, the amount of energy spent running mining hardware goes up. The barrier of entry to competing on these currencies is twofold; you need mining equipment and you need to continually pay for electricity.

Recently, however, more cryptocurrencies are migrating to, or launching as, proof-of-stake. Traditionally, proof-of-stake pays out block rewards based on a set annual percentage rate (APR) in the parameters defined by the developers of the coin. Some more recent projects have opted to reward a static amount per block. Since most wallets don't support offline staking, it is critical that not only is your wallet online but the connection and computer hosting it is stable and reliable. Currencies using PoS include NXT, peercoin, PIVX and soon Ethereum.

Proof-of-stake currencies and masternodes both reward primarily on the value of the wallet. These wallets help maintain the integrity of the entire currency while masternodes perform more computational-critical roles. Getting a noticeable return on vestments (ROI) in proof-of-stake currencies requires a lot of initial investment. That investment is locked into a single currency. Many of these currencies do not support offline staking, so the wallet would be required to have as high an uptime as possible for it to remain competitive enough to receive block rewards.

Managing all of these currencies and keeping track of trading, buying, and selling is a daunting task for people that cannot do this full-time. MASS Cloud Ltd. bridges the gap between ease of use and currency fluidity. Our platform performs the trades, buys and sells on select coins, and automatically converts block rewards to Ethereum when paid out.

MINING

The type of hardware and cost of operation varies on the cryptocoin. Bitcoin started off on CPU miners, then was overtaken by high-end AMD video cards, and now it is overwhelmingly controlled by specialized ASIC hardware. These ASIC miners can run over a thousand dollars for a single high-powered unit[1] and power supply[2]. This unit offers 13.5 terahash per second and recommends a 1600-watt power supply. Using an online calculator[3], we can see our return on investment given the specifications of the miner, power usage, energy cost, and expected growth rate of 10.25% every 2 weeks.

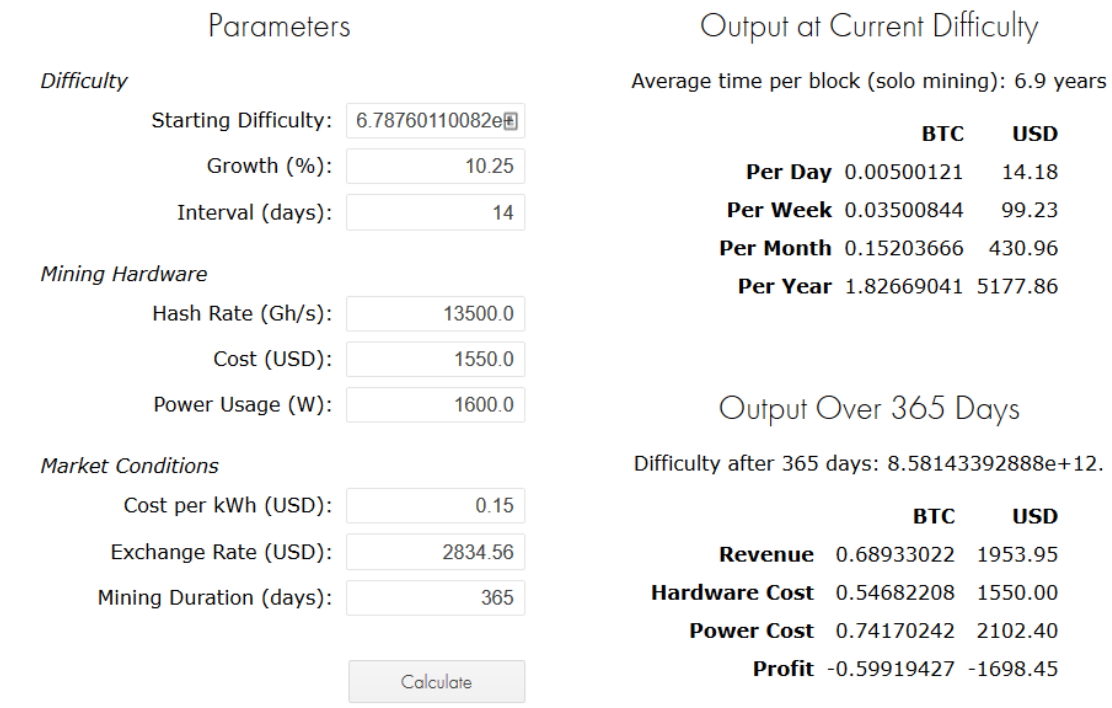

Figure 1 - Bitcoin Mining Parameters

[1] https://shop.bitmain.com/productDetail.htm?pid=00020170607035948018mhO6CJXR068E Antminer S9 - $1200
[2] https://www.evga.com/products/product.aspx?pn=120-G2-1600-X1 EVGA 1600w PSU - $334
[3] http://jblevins.org/btcmpc/

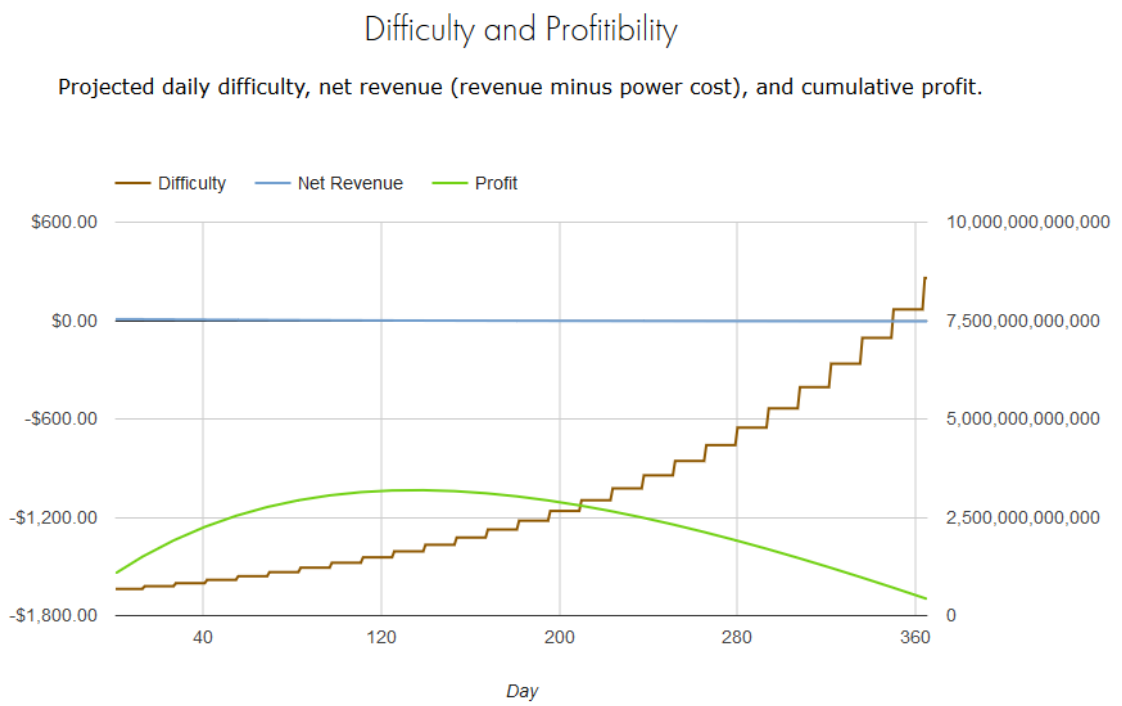

Figure 2 - Bitcoin Mining Returns

With one unit and the steady rise of difficulty, you would never pay off the initial investment. This can be extrapolated to any number of these machines; the rate at which the difficulty raises outpaces the profit. Bitcoin would need an ever-increasing rise in demand for the return to come close.

Mining Ethereum is still profitable after several months on a modest investment. This is all going to change in the near future when Ethereum moves to proof-of-stake[4]. The details of their PoS implementation have not been finalized yet, so the cost of entry is still undetermined.

For example, in order to run and maintain your own Dash masternode (a popular PoS/Masternode cryptocurrency), you must have at least 1000 Dash[5] in a wallet at all times. Dash currently trades for around $150[6], which means an initial investment of $150,000 is needed to start a masternode on the Dash blockchain. This does not include the cost of hardware, or securing the wallet against attack.

[4] https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[5] https://www.dash.org/masternodes2/
[6] https://coinmarketcap.com/currencies/dash/

MASS CLOUD LTD.

MASS Cloud Ltd., a Hong Kong-based company, manages the high cost of entry in proof-of-stake and masternode currencies, difficulties in keeping the wallets filled and online at all times, and managing trades between currencies to prevent over funding a single one. We are a team of career professionals with backgrounds in Fortune 300 companies. We believe in the idea of making cryptocurrency less resource intensive by using proof-of-stake implementation, and are bringing what it offers to the public by reducing the cost of investment and complexity in monitoring multiple currencies over multiple exchanges. Our backgrounds are in software engineering, security, virtualization, cluster computing, high-availability ecommerce front ends and back ends, as well as continuous monitoring, trading, and advising on newly announced currencies and ICOs.

Our goal is to provide a new method of investing fiat currency into a continuously growing fund of cryptocurrency fund that pays out block rewards automatically and fairly across all token holders. We are a company that is taking all of the nuances of investing into different cryptocurrencies, and bringing it together in a simple, coherent and secure platform. Because of our faith in this project, we are locking our share of the MASS tokens for 1 year. Also during that period, we will be unable to trade or transfer the tokens received as part of the ICO[7]. The rewards from those shares will go back into the pool to help increase the size of the underlying assets held by MASS. This will increase the number of rewards holders receive. This has a twofold effect which heavily benefits all token holders during this time: 1) increased rewards while staking, and 2) increased value for the MASS token itself, because the underlying assets are also increasing. By the end of the 1 year locked period, we project that the fund will be in a stable growth that MASS Cloud Ltd.'s employees can begin to receive payouts from their shares.

TRANSPARENCY & TRUST

We want to be as transparent and open as possible, while also offering the most security for all token holders. All wallets under the control of the team will be multi-signature wallets to ensure a higher level of security and accountability. Once the ICO ends, the remaining funds (after we receive our 10% share), will be transferred to a new smart contract that will act on behalf of the pool. This contract will perform the following actions:

- Publish outgoing Ethereum addresses with a waiting period of one week before funds are sent.
- Publish all staking and masternode wallet addresses along with their transactions to both the blockchain and our website.
- Publish all exchange wallet addresses along with their transactions to both the blockchain and our website.
- Transactions above 30% of the entire pool will have a waiting period of one week before being released.
- Announce and approve a list of new coins to invest in that the MASS token holders voted on.
- Rebalance currencies to ensure no more than 30% of the pool is invested in a single currency.
- Currencies that have a 200%+ return when rebalanced will reward all token holders a share of 10% of the return.
- Prevent Ethereum transactions to unapproved addresses.
- Keep a public record of all outgoing expenditures as all transactions can be tracked.

[7] https://github.com/mass-ltd/MASSToken/tree/master/contracts

- Create a kill switch that will liquidate all currencies, converts to Ethereum, and release the funds to all token holders. This will only be invoked in case of emergencies

THE TEAM

Clinton McLeay

https://www.linkedin.com/in/clinton-mcleay-09688153/

Clinton McLeay is an entrepreneur, systems, and user experience expert. With almost 25 years of experience in computing, system security, and Linux based systems, Clinton has built custom solutions for a varied selection of clients; from Fortune 500 companies such as MASCO and MGM Grand, to government organizations such as The City of Southfield in Michigan, to musicians like Ozzy Osbourne. Clinton has a great passion for learning anything technology related and is able to identify future trends with great accuracy.

Kris Borodiansky

https://www.linkedin.com/in/kristopher-b-331b42100/

Kris Borodiansky is a seasoned developer demonstrating proficiency and expertise in a broad range of programming languages. He has nearly 25 years of experience in computing, UNIX-based systems development and administration with his biggest passions being blockchain development and overall improvement of the quality of life through technology. For over 6 years now, he has played vital roles in various blockchain-based projects providing expert consult and development services. He was the first to innovate and bring additional useful utilities to the standard crypto wallets as they're known today and he works passionately continuing development within the crypto space.

Dennis Klungler

https://www.linkedin.com/in/dennis-klungler-9b387715/

Dennis Klungler is a systems administrator with over 20 years of experience in server administration and process automation. Complimented by his programming background in platform development for several international companies, he has the knowledge and experience to identify and resolve issues across the board. He started mining Litecoin in 2013 with 50 GPUs spread over 10 mining rigs, and has been involved in cryptocurrencies ever since.

Kurt Knudsen

https://www.linkedin.com/in/kurt-knudsen-5265691/

Kurt Knudsen graduated with a BS in Computer Science from the University of South Florida in 2005. From there, he went on to get his MS in Interactive Entertainment. He took the dive into game development for a short bit before going on to more software development and server-oriented roles at various companies. He has used his skills as a writer and engineer to work on documenting global projects that continue to evolve to this day, physical server building and maintenance, Windows and *NIX-based development and security, and automating application deployment across hundreds of servers. With experience in multiple languages, he jumped at the chance to dive into Ethereum development.

MASS ICO DISTRIBUTION

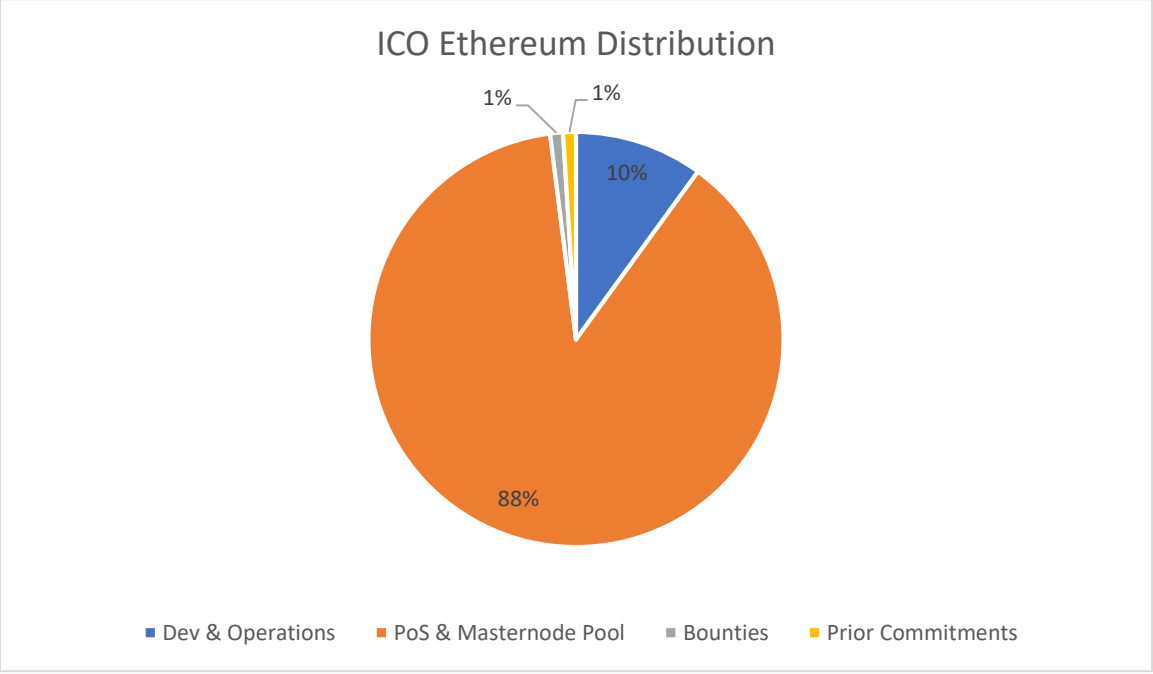

Figure 3 - Ethereum Distribution

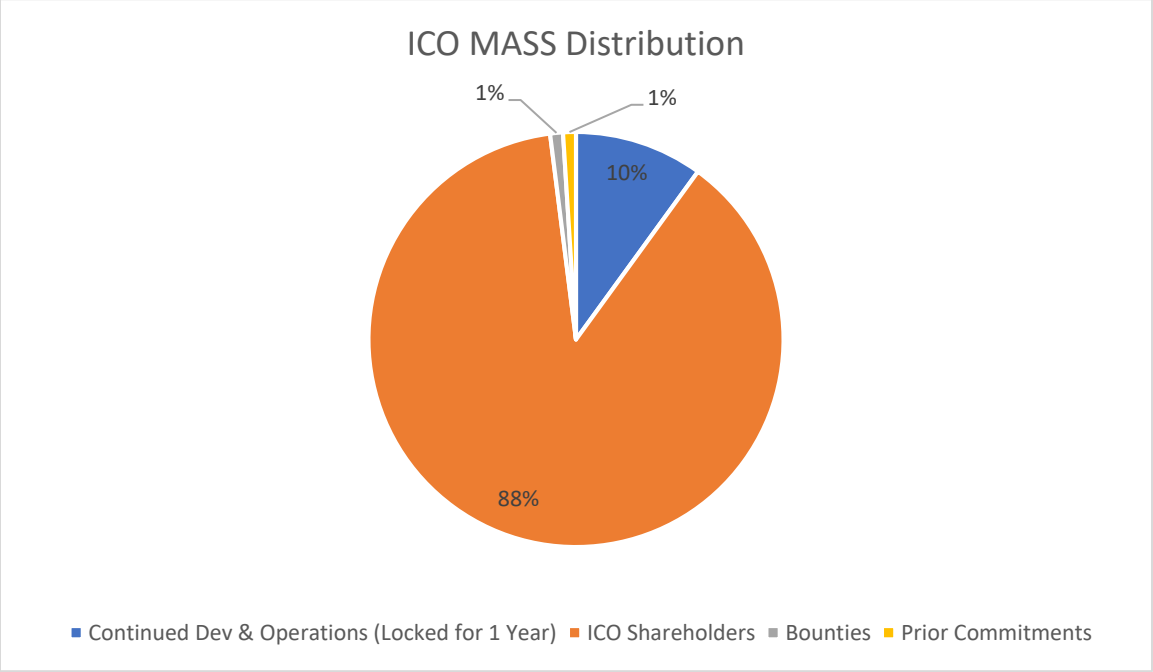

Figure 4 - MASS Distribution

The above pie charts describe the distribution of Ethereum and tokens after the ICO. The percentages represent the total quantity of MASS tokens sold. This means that 88% of the funds raised during the presale and the ICO will be used to invest in other digital currencies. 2% of total Ethereum and MASS are split between bounty programs and prior commitments.

MASS TOKENS

MASS tokens are purchased at an exchange rate of 1000 tokens per Ethereum. During pre-sale, purchases are given 30% more tokens until it closes 7 days later or reaches its cap of 10 million tokens. Once the ICO starts, purchases during the first 5 million tokens will receive 20% more and tokens purchased during the next 10 million will receive 10% more, purchases made after the 2nd phase ends will receive no bonus. The tokens are locked during the presale and the ICO and will be released upon the completion of the ICO. There is a cap of 61 million MASS tokens in total.

The following flowchart helps visualize the structure of the contract and pooling system:

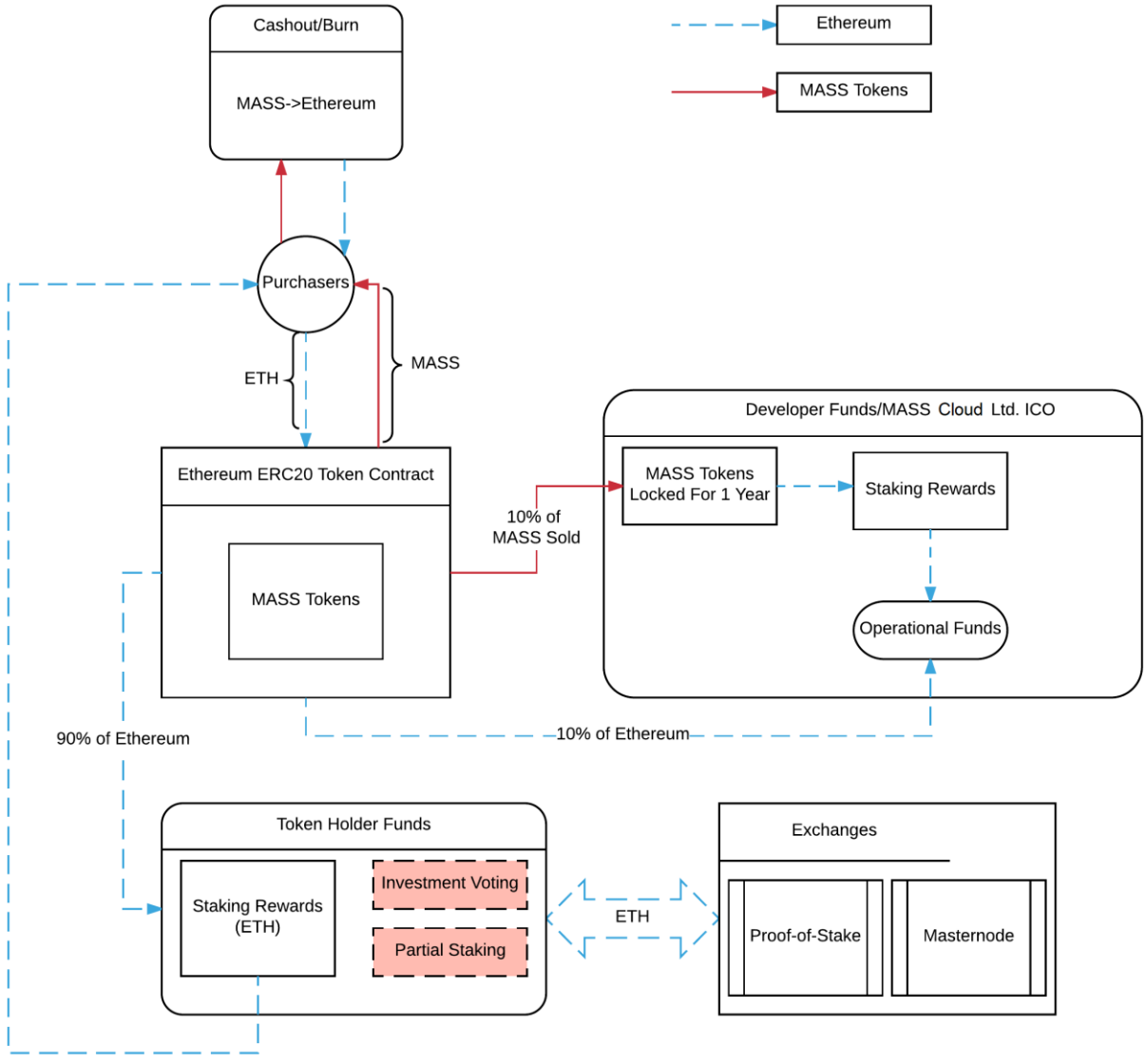

Figure 5 - MASS Token Flowchart

1. Tokens are purchased by sending Ethereum to the contract. The exchange rate is based on how many tokens have been sold and can be seen in the contract source.[8]
2. After sending Ethereum, the contract allocates MASS tokens to the sender's address.
3. Once the ICO ends, token holders can send a message to the contract to stake their tokens.
4. Staked tokens cannot be transferred, traded, or burned.
5. These staked tokens will give holders a fair payout of rewards.
6. Unstaked tokens can be traded, sold or burned, but their shares of the rewards are reinvested into the pool.
7. Burning tokens will give the owner a fair percentage of the total Ethereum value of MASS Cloud Ltd., minus a burn fee to prevent abuse and market manipulation as well as manual oversight.

Once the ICO ends and the funds are released to a wallet controlled by our back end system, they will be invested into multiple supported currencies and masternodes. Regardless of if tokens are staked or not, their Ethereum equivalent will be put to use by the pool. Block rewards are paid out based on the amount of MASS staked for each owner and the amount of time the tokens spent being staked.

$$blockReward = \frac{stakedMASS}{totalMASS} * \frac{stakedBlocks}{totalBlocks}$$

If tokens are unstaked between rewards, their share decreases and the remainder goes back into the pool. This is to prevent token owners from only staking right before a block reward is expected to pay out. The following formula shows the ratios between them.

$$poolReward = \left(\frac{stakedMASS}{totalMASS}\right) - \left(\frac{stakedMASS}{totalMASS} * \frac{stakedBlocks}{totalBlocks}\right)$$

To put this to use, let's take the following example. Bob owns 1000 MASS tokens. The total MASS of the pool is 10,000 MASS. Bob was staked for 25 out of the 28 blocks between rewards.

$$bobReward = \frac{1000}{10000} * \frac{25}{28} = 0.0893$$

Bob gets 89.3% of their expected share. The remainder goes into the pool:

$$poolReward = \left(\frac{1000}{10000}\right) - \left(\frac{1000}{10000} * \frac{25}{28}\right) = 0.0107$$

The pool receives 10.7% of the reward to not only boost the value of the pool, but to also reinvest these rewards into new coins and masternodes.

Tokens that are lost and are not staked will not have a negative impact on the pool, since unstaked tokens receive no reward. Staked tokens will always receive their share of block rewards until they are marked as unstaked.

[8] https://github.com/mass-ltd/MASSToken/tree/master/contracts

BONUS STRUCTURE

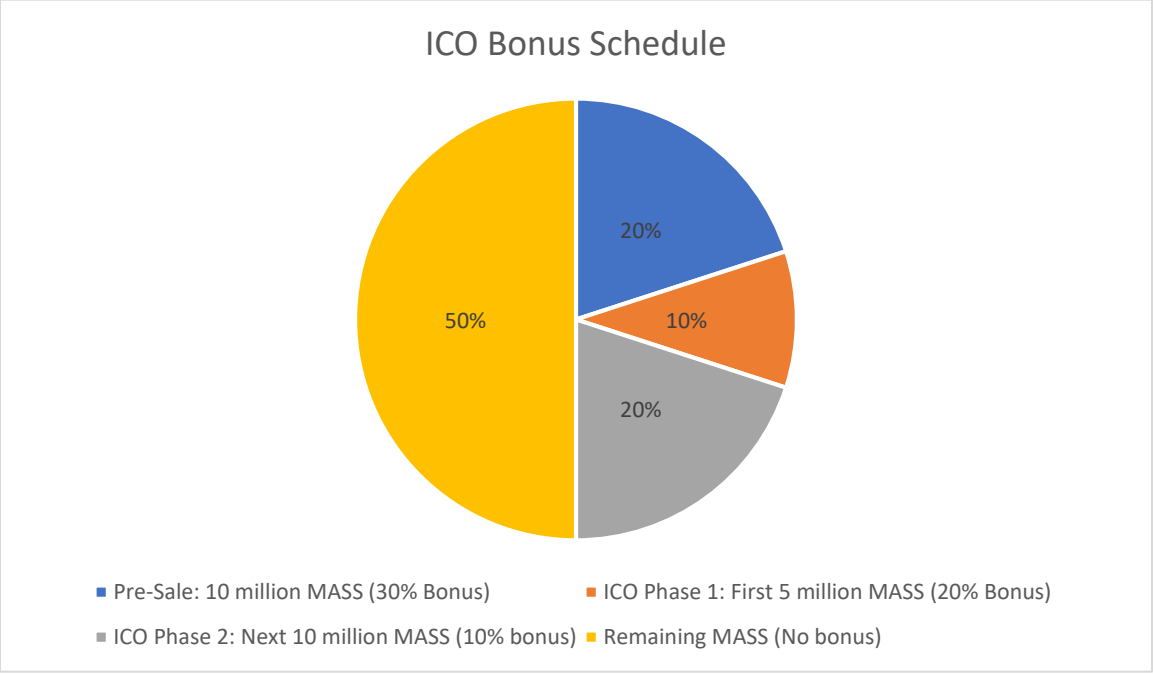

Figure 6 - ICO Bonus Schedule

During presale and the ICO, purchases can receive extra tokens up to a certain limit[9]. We are setting a cap of 10 million tokens to be sold during the presale. During this time, all purchases will be given 30% more tokens. Once the ICO starts, the bonus structure will change to the following:

- Phase 1 of the ICO will offer 20% more tokens on purchases on the first 5 million tokens. This is outside of the tokens sold during the presale.
- Phase 2 of the ICO will offer 10% more tokens on purchases on the next 10 million tokens.
- Phase 3 of the ICO will offer no bonus tokens and a flat exchange rate of 1000 tokens per Ethereum is set.

INVESTMENT VOTING

Investment voting is part of our road map, and will be implemented in the near future outside of the original contract. Voting will initially work by allowing token holders the opportunity to vote on supporting new coins. Future improvements will allow token holders to choose where their share of Ethereum is invested. If token holders choose to have their share staked into a single currency, they only get rewards from that currency. Their share of the reward is based on the above formulas, but only to that specific currency and not all investments combined. The rewards could be higher or lower depending on multiple factors, including the number of Ethereum staked, and stability and growth of the coin. This feature will reward token holders that see potential in a supported coin by allowing them to have a greater stake in it.

[9] https://github.com/mass-ltd/MASSToken/tree/master/contracts

POTENTIAL COINS

An example set of supported coins and their current market value[10], as of June 12, 2017, are:

Name	*Ticker*	*Value (USD)*	*ROI (6/2016-6/2017)[11]*
BlackCoin	BLK	$0.448	145.86%
Magi	XMG	$0.127	-
Mintcoin	MINT	$0.000236	797.89%
ReddCoin	RDD	$0.0022	8,290.29%
NeosCoin	NEOS	$3.08	**11,875.46%**
Crown	CRW	$0.838	-
PIVX	PIVX	$1.43	**13,143.41%**
Stratis	STRAT	$8.60	**81,163.31%**
TransferCoin	TX	$0.416	4,753.08%
MonetaryUnit	MUE	$0.077	**26,271.78%**
VeriCoin	VRC	$0.526	914.46%
Nexus	NXS	$0.821	2,596.45%

New coins will be added as time goes on; and when investment voting functionality is implemented, token holders will be a major part of vetting potentially successful coins.

AUTOMATION

One of the major benefits of using MASS is our ability to automate a large portion of the process. We have years of experience in automation with tools like ansible on platforms such as Amazon's AWS. Our back end will automate the process of reward payouts, currency exchanges, auto-balancing of investments, managing masternode instances, and account address verification with blockchain messages. We fully plan on taking suggestions and recommendations from token holders to help improve our platform.

[10] https://coinmarketcap.com/currencies
[11] http://www.cryptocurrencychart.com

SECURITY

One of the most difficult parts of running a successful masternode is securing the server it runs on. MASS is using enterprise-grade service providers that offer DDoS protection, VLANs, and multi-factor authentication (MFA). On top of that is our decades of experience as high-level network and systems administrators. Our plan is to have the masternodes on a private network with dual failover VPNs to a DDoS protected public IP. Should the primary address go down, the VPN will change traffic to a new DDoS protected public IP so there is no downtime.

To manage your tokens, you will be able to register an account at www.mass.cloud and attach your Ethereum address to it. In order to control access to your account through our site, you will have to send a challenge message to the blockchain. Verified addresses will be cryptographically signed in our database with our wallet's private key. This ensures that no one can gain access to your account. Even in the unlikely event of a hack, the attackers won't be able to properly sign the new Ethereum address.

Along with a standard username/password, users will be asked to enter in a master passphrase or PIN that will only be used to burn their tokens, or to transfer tokens to another address. The purpose of this is to protect against unauthorized access to your accounts, even by us. This secondary passphrase/PIN will also be signed by our private key for another layer of security.

ROAD MAP

Our plans for the immediate future are investor voting and partial staking. We will create and publish new smart contracts that utilize these features, and will rely on the authenticity of the original contract to continue to control the distribution of MASS. We will adopt our framework to integrate with new coins and exchanges as they come online. A full-features road map will be available on our website once the details are locked down, and we begin to work on them.

SUMMARY

MASS Tokens are the first of its kind that will likely be the standard in how people invest in cryptocurrencies. MASS Tokens allow token holders the ability to stake securely in multiple currencies and masternodes simultaneously, while receiving block rewards automatically. Due to their unique situation, MASS Tokens hold twice the value of typical ERC20 tokens. Not only can they be traded on various exchanges around the world, but the tokens themselves lead to a large pool of funds receiving block rewards on a continuous basis, which will drive their value on exchanges even further.

GLOSSARY

Ansible: An open-source automation engine that automates software provisioning, configuration management, and application deployment.

APR: An annual percentage rate is the interest gained on an investment over a one year period.

ASIC: Application-specific integrated circuit is an integrated circuit customized for a particular use, rather than for general-purpose use.

Back end: Denotes a subordinate processor or program, not directly accessed by the user, which performs a specialized function.

Block: Where transaction data is permanently recorded into files, like a stock transaction ledger. Each block contains a timestamp and a link to a previous block. Blocks are organized into a linear sequence over time (also known as the blockchain).

Blockchain: A distributed database that is used to maintain a continuously growing list of records, called blocks. They are inherently resistant to modification of the data.

Burned, burning: A function that is built into the smart contract that allows token holders to quickly liquidate their share of the MASS pool funds and have them converted to Ethereum and sent to them.

Cryptocurrency: A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

DDoS: Distributed Denial of Service is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.

Ecommerce: The buying and selling of goods and services, or the transmitting of funds or data, over an electronic network (primarily the internet).

ERC20: A token standard that describes the functions and events that an Ethereum token contract has to implement.

Ethereum: An open-source, public, blockchain-based distributed computer platform featuring smart contract (scripting) functionality, which facilitates online contractual agreements.

Failover VPN: Virtual private network tunnels automatically and seamlessly fail over to a backup external interface if a failure occurs, resulting in no downtime.

Fiat currency: Legal tender whose value is backed by the government that issued it.

Front end: The presentation layer between the user and the back end.

Hash, hashes: The values returned by a hash function, which is any function that can be used to map data of arbitrary size to data of a fixed size.

ICO: Initial coin offering is an unregulated means by which funds are raised for a new cryptocurrency venture.

MASS: Masternode and Staking Service is an Ethereum token (ERC20) that is backed by a diverse pool of proof-of-stake and masternode cryptocurrencies using a smart contract that allows holders to receive block rewards from the pool of cryptocurrencies in the form of Ethereum.

Masternode: Servers that facilitate certain vital network functions of a cryptocurrency that uses them.

MFA: Multi-factor authentication is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism.

PoS: Proof-of-stake is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus.

ROI: Return on Investment measures the amount of return on an investment relative to the investment's cost.

Sign, signed: A digital signature that is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit.

Smart contract: Computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary.

Stake, staked, staking: The process of specific cryptocurrencies that reward you for holding them, more formally called proof-of-stake minting. For MASS, this process securely locks your tokens into a staking smart contract which lets you receive the block rewards from the various cryptocurrencies in Ethereum.

Terahash: 1,000,000,000,000 hashes, usually mentioned in the context of cryptocurrency mining equipment, as a number like 10 TH/s. This means the equipment is able to perform 10 trillion hashing operations per second.

Unstake, unstaked, unstaking: When the user opts out of future block rewards and unlocks your tokens. While unlocked, the mass pool uses these funds to grow the size of the pool.

Uptime: The measure of the time a computer/server/machine has been working and available.

VLAN: A group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. As VLANs are based on logical instead of physical connections, they are extremely flexible.

VPN: A virtual private network creates a secure, encrypted connection that extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Wallet: A secure digital wallet used to store, send, and receive cryptocurrencies. Any Ethereum ERC20 compatible wallet will work with MASS.