



**

ION white paper v. 0.1

<https://github.com/ionomy/ion/wiki/ION-Technical-Whitepaper>

April 9, 2016

ION white paper v. 0.1

Adam Matlack adam@ionomy.com

Michael Pfeiffer michael@ionomy.com

Michael Pfeiffer michael@ionomy.com

**
**

Richard Nelson
richard@ionomy.com

**
**
—

This "living document" will be updated and revised until published upon public launch of ION.

Abstract

ION is a blockchain based decentralized cryptocurrency that rewards network participation via static proof of stake. ION rewards "connectivity age" instead of "coin age," thus eliminating abuse from exchanges and users that do not actively contribute to the network. By having a static reward system, the rewards for participation are proportional to the work every active node contributes. This discourages centralization and promotes network health. In addition to static rewards, ION implements a masternode network to incentivize large holders, and perform advanced functions such as near instant and private transactions.

This paper describes the basic coin specifications, features, and capabilities of the coin. The paper also describes coin distribution, funding purposes, future growth efforts, and the involvement of ionomy.com.

The long term vision for ION is a thriving cryptocurrency ecosystem centered on gaming and digital goods.

![Authors](http://i.imgur.com/MIT78gw.png)

Table of contents

- [Abstract](#)
- [Table of contents](#)
- [Coin overview](#)
- [Proof of work vs. Static proof of stake](#)
- [Initial coin supply](#)
- [Block reward schedule](#)
- [Distribution of coin](#)
- [Blockchain specifications](#)
- [Staking wallets](#)
- [Masternodes](#)
- [Private transactions](#)
- [Coin development roadmap](#)
- [Bounties](#)
- [Coins in Context](#)
- [Conclusions](#)
- [Acknowledgements](#)
- [References](#)
- [Sample ION Block](#)

Coin overview

- **Static proof of stake, version 3**
- **Initial coin supply: 10,900,000 IONs**
 - 5 million IONs will be available through the Initial Coin Offering (ICO) in exchange for BTC and a wide selection of other cryptocurrencies.
 - 3.4 million IONs are allocated to ionomy.com and shall be distributed as structured incentives to gamers through the gaming applications designed by ionomy.com.
 - 2.5 million IONs are reserved to pay bounties for coin development.
- **Block rewards**
 - Year 1 = 23 IONs per block
 - Year 2 = 17 IONs per block
 - Year 3 = 11.5 IONs per block
 - Year 4 = 5.75 IONs per block
 - Years 5 to 9 = 1.85 IONs per block
 - Years 10 to 100 = 0.2 IONs per block

- Year 1 = 25 IONs per block
- Year 2 = 17 IONs per block
- Year 3 = 11.5 IONs per block
- Year 4 = 5.75 IONs per block
- Years 5 to 9 = 1.85 IONs per block
- Years 10 to 100 = 0.2 IONs per block

- **Final coin supply: 55 million total coins**

- **Blockchain specifications**

- Target block generation time: 1 minute
- Block height: 1 kb to 8 mb

- **Masternodes**

- 20,000 IONs transaction with 15 block confirmations
- Peer validated network uptime
- Private transactions (0.01 ION fee to masternodes)
- Active masternodes proportionally receive 50% of each block reward.

- **Staking wallets**

- Connected wallets rewarded proportional to network uptime and coin volume

- **Coin development roadmap**

- Specified rewards engage talented developers to improve coin functionality
- Developers paid when code is validated to meeting bounty specifications and is merged into the ION core code on github

Proof of work vs Static proof of stake

Bitcoin achieved the first distributed blockchain-based transaction ledger and an immutable digital currency. To achieve this, Bitcoin rewarded the distribution of computing equipment to maintain a decentralized blockchain and secure network. There was a short period of time when this worked well, but now Bitcoin rewards the *accumulation* of computing power, and only a few consolidated pools maintain the network.

The rapid growth of the Bitcoin network is also a disastrous burden on ecology. The exponential expansion of computing power has lead to a similar rise in difficulty, and power hungry mining consume a vast amount of electricity.

This concentration of power threatens the distributed model of checks and balances, and even governance over core development is at odds with how to solve the growing problems. A single transaction confirmation can take in excess of 12 minutes (blockchain.info, 2016) and the technology is vulnerable to attacks increase the delays.

Thus, ionomy.com rejected mining and proof of work as the basis for security and adopted proof of stake instead.

Critics of proof of work developed proof of stake (PoS) as an alternative protocol. PoS systems depend upon a low-energy, distributed computing network to achieve the same ends of a secure, distributed blockchain. They rely on accumulation of coin instead of computing power as the basis for rewards for securing the network.

Early models of proof of stake were designed around "coin age," the length of time that the coin was held in a wallet, and "coin weight," the total amount of coin in the wallet. These have proven to be necessary but insufficient conditions for rewards because they do not reward active facilitation of network transactions. In theory, and in practice, holders of cryptocurrencies based on the first versions of PoS could deposit large volumes of coin into a wallet, take it offline, accrue coin age for an extended period of time, then bringing the wallet online momentarily to obtain an instantaneous reward.

This first version of PoS rewards users for holding onto coins without actively contributing to the integrity of the network. In this model, exchanges and other large holders of coin maintain offline wallets, and only periodically connect them to the network to generate and sell the stake. This directly increases the coin supply while driving down the market value of the coin.

In contrast, ION uses a "static" proof of stake system, version 3 (PoS 3, or SPoS), which aligns incentives with user behaviors to actively contribute to a robust, fast, and secure network. The reward is "static" because it is always the same (50% of the block reward). Coin weight still matters, but "connectivity age," – the duration a wallet maintains active network communication – replaces coin age as the primary probability parameter for staking. Rewards are thus contingent upon active work and the amount of ION held in wallets to maintain and secure the network.

In addition, ION implements masternodes (Duffield, 2015) to reward large holders of coin, contribute to network robustness, and perform advanced functions such as near instant and private transactions.

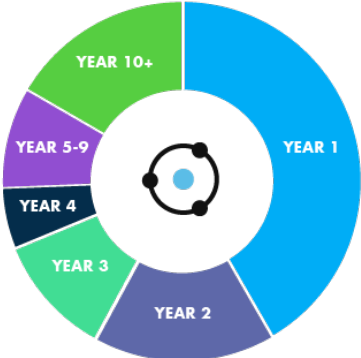
advanced functions such as near instant and private transactions.

Initial coin supply

A total of 10,900,000 IONs will be used for the initial coin supply. These coins are generated in the genesis block and will be held in trust by ionomy.com. The coins shall be distributed as follows:

- 5 million IONs will be available through the Initial Coin Offering (ICO) in exchange for BTC and a wide selection of other cryptocurrencies. Details about the ICO and cost can be found at ionomy.com. ionomy.com will manage the proceeds from the ICO and any coins that are not sold will be used to incentivize independent developers to integrate their games into ionomy.com.
- 3.4 million IONs are allocated to ionomy.com and shall be distributed as structured incentives to gamers through the gaming applications designed by ionomy.com. These incentives are meant to help distribute the coin, grow the user base, and engage users in the ION social, financial, and gaming economy.
- 2.5 million IONs are reserved to pay bounties for coin development. Bounties contribute to decentralized development. They invite cross-fertilization across the crypto space, bringing the best minds to contribute to the ION economy (the "ionomy"). Bounties also allow the community to drive initiatives by posting rewards for any feature desired. Initial development priorities are outlined in the *Bounties* section below.

Block reward schedule

	Year	IONs/Block	IONs//Year	Total
	1	23	12,000,000	22,900,000
	2	17	9,000,000	31,900,000
	3	11.5	6,000,000	37,900,000
	4	5.75	3,000,000	40,900,000
	5-9	1.85	1,000,000	45,900,000
	10-100	0.2	100,000	55,000,000

Distribution of coin

Many alternative cryptocurrencies start with a proof of work phase. Developers reason that miners become engaged with the coin economy and earn the coin through the work of mining. The lesson the ionomy.com team has taken from the history of cryptocurrency, however, is that the PoW phase encourages "mining and dumping" which drives down the value of the asset from the start. This supposedly "engaged" user base simply uses mining as a vehicle for quick profit then leaves without contributing ongoing value to the coin or community that uses it.

The ionomy.com business plan, however, is designed to grow the coin value through partial centralization in order to nurture a community whose continuous use of ION gives the coin lasting transactional value. For fuller details on the business model, please see the [ionomy.com white paper](#).

Distribution of IONs takes place both through the ION technology and through the ionomy.com gaming company, according to its business plan. On the technology side, IONs are distributed as a reward for network security and blockchain maintenance performed by wallets and masternodes holding IONs. On the business side, ionomy.com rewards participants on the ionomy.com investment and social platform and rewards gamers on the gaming platforms for their investments, engagement and contributions to the ION community. This joint mode of distribution safeguards the technological infrastructure and populates the ION economy with an active user base. The plan is designed to generate a continuous stream of ION users and to give the coin lasting transactional value. For fuller details on the business model, please see the [ionomy.com white paper](#).

Blockchain Specifications

- Target block generation time: 1 minute
- Block height: 1 kb to 8 mb
- Fee for private transactions: 0.01 ION
- Static proof of stake version 3
- See [Appendix A](#) for sample ION block

State proof of stake version 2

- See [Appendix A](#) for sample ION block

The combination of one minute block time and minimum transaction fees were designed with speed and security in mind. The ample block height allows for scaling as network transaction volume increases. Collectively, these specifications prevent malicious actors from flooding the network with fake transactions, as has happened lately bringing Bitcoin transactions to a crawl (Gautham, 2016). Bad actors can still try to fill large blocks with multiple small transactions, but they will waste their time and money. The masternodes will collect large fees from their failed efforts.

Staking wallets

QT wallets have been developed for general users. Daemon wallets have been developed for advanced users. Wallets will be maintained for all major desktop platforms: Windows, Mac, and Linux. QT and daemon wallets give ION holders complete control of the security of their ION, with controls to send and receive transactions. Online wallets contribute to network security by confirming successive blocks of validated transactions as they are added to the official blockchain, thus maintaining the complete ledger of all ION transactions.

- Coins required: No minimum. (Wallets must contain a non-zero sum of IONs to receive stake rewards.)
- Wallet stake reward = 50% block reward for each discovered block.

Staking is probabilistic, and probability is distributed according the amount of ION in the wallet address (coin weight) and the duration ION is held in the continuously connected wallet (connectivity age). Valid network connectivity requires that the wallet be connected to the internet with a sufficiently high-speed, stable connection to support the blockchain.

Previous versions of Proof of Stake require what is known as checkpointing. Checkpointing is a centrally broadcasted full node that is signed by the developer and is designed to help verify coin stake before it is accepted into the block tree. In ION, every node is a full node, and because of this no checkpoint system is needed. By removing this partial centralized dependency that existed in previous PoS versions, all nodes are fully authorized and makes a network attack far more difficult.

Masternodes

####Secure public and private transactions

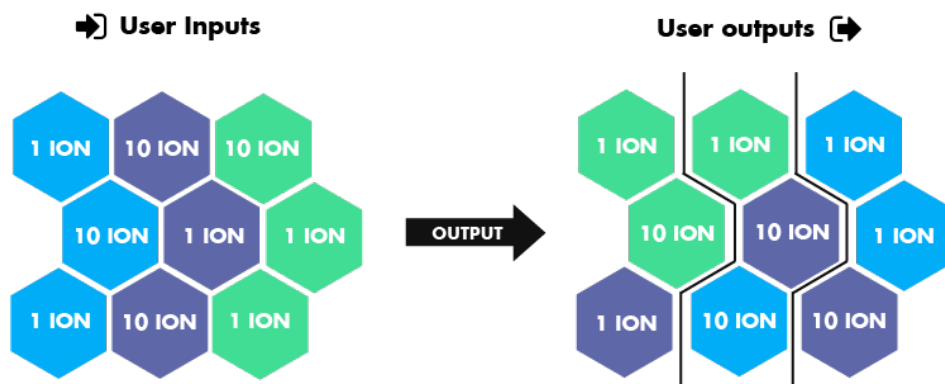
Masternodes validate all public transactions within about 4 seconds by communicating each transaction across all nodes on the network to prevent double spending (Duffield, Schinzel, and Gutierrez, 2014). When private transactions are initiated, masternodes also perform the work necessary to make the transactions hard to trace. The masternode network will be able to perform additional functions as new developments are commissioned and the bounties executed.

Masternode specifications

- Coins required: 20,000 (minimum and maximum)
- Reward: 50% of the block reward + all fees for transactions contained in the block
- Peer validated network uptime

Private transactions

Masternodes facilitate private transactions through a decentralized mixing service that takes advantage of the perfect fungibility of the currency. Any unit of ION has the equivalent value to any other unit of identical size, regardless of the transaction history of any particular unit. Masternodes use this property to automatically break up private transactions into multiple identical and indistinguishable transactions, both adding complexity to the original transaction and obfuscating the provenance of any given unit.



***Each color represents one user's transactions

*Diagram 2: In this example of a block of transactions, three users submit funds in various set denominations. **Users pay themselves back in the form of new outputs, which are randomly ordered. *

Private ION transactions are initiated through a local wallet and received by the masternode subnetwork. Transactions are processed in groups of three. Inputs of common denominations are required – for example 0.1 ION, 1 ION, 10 ION, or 100 ION.

Upon application to the mixing pool, a receiving masternode propagates the transaction set throughout the network. If only one or two

*Diagram 2: In this example of a block of transactions, three users submit funds in various set denominations. **Users pay themselves back in the form of new outputs, which are randomly ordered. *

Private ION transactions are initiated through a local wallet and received by the masternode subnetwork. Transactions are processed in groups of three. Inputs of common denominations are required – for example 0.1 ION, 1 ION, 10 ION, or 100 ION.

Upon application to the mixing pool, a receiving masternode propagates the transaction set throughout the network. If only one or two private transactions are pending, they are held in queue until three are in the mixing pool. Fees are extracted from the individual transactions, then charged collectively to further obfuscate the transaction history.

Private send is limited to 20,000 ION, thus requiring multiple sessions to thoroughly delink associated transaction history from significant amounts of money. Since each session is limited to three clients, an observer has a one in three chance of being able to follow a transaction.

Mixed transactions are chained together through multiple masternodes, making traceability exponentially more difficult with each additional chained transaction. Users have some control over the degree of mixing. More mixing takes more time, but more thoroughly obfuscates inputs. The fee for these transactions grows with each degree, as the process is more labor intensive for the masternodes (Duffield and Diaz, 2015).

This method of mixing is a trustless, integrated, on-chain, on-network service that is efficient, effective, and safe. It is initiated directly within a local wallet and completed without leaving the ION network. While some details of private transactions are obscured, the system nevertheless retains verifiable integrity of spent coins on the ION blockchain.

What is the incentive to run a masternode?

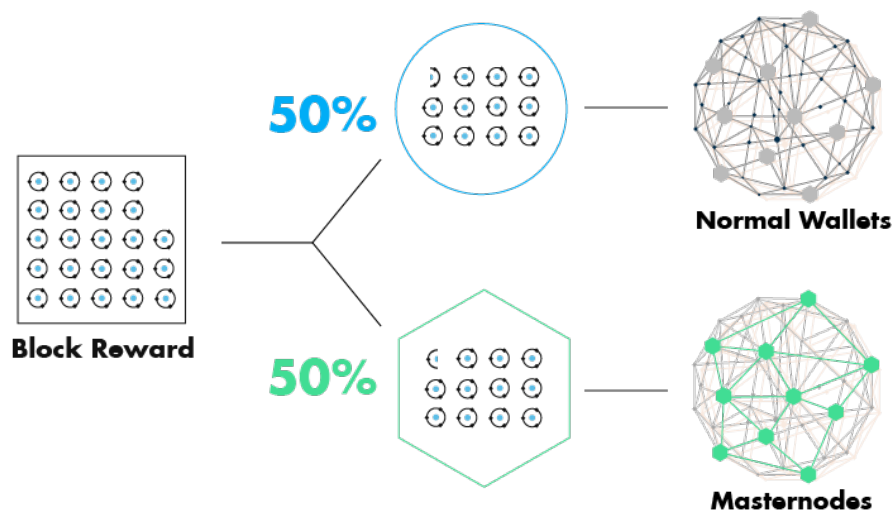


Diagram 3: Average daily reward $\approx (\# \text{ of blocks per day} * \text{block reward} * 50\%) / (\# \text{ of masternodes})$

Masternodes receive fixed rewards (50% of the block reward) which are probabilistically distributed among peer validated masternodes. Masternodes recursively scan peer node performance, and only high performance nodes with sustained, stable, high-speed internet connections are eligible for rewards. In addition to receiving 50% of the block reward, a masternode receives all fees for public transactions completed in a block and for all private transaction pools initiated in the block. These incentives promote continuous connectivity to maintain a high performance network.

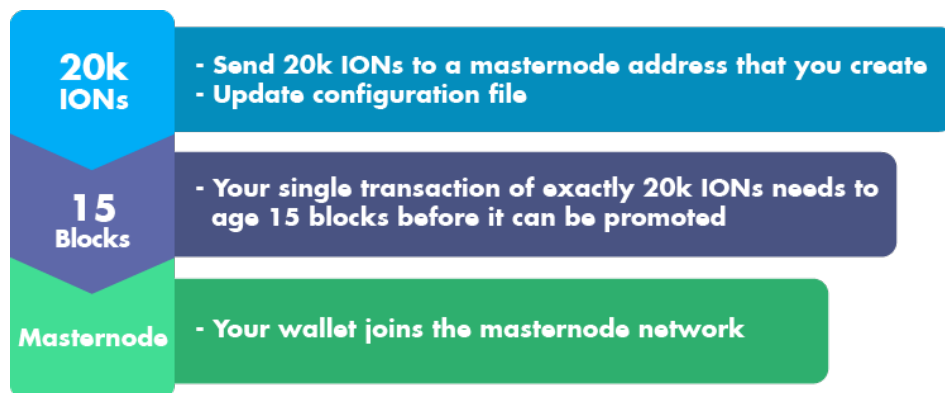


Diagram 4: Procedure to activate a masternode.

In theory, malicious actors could also run ION masternodes, but not provide any of the quality service that is required of the rest of the network. To reduce this possibility and discourage people from using the system to their advantage, all nodes must regularly ping the rest of the ION masternode network to ensure they remain active. This work is done through a selection of 2 quorums per block. At every new block hash, Quorum A checks the service of Quorum B. Quorum A are the closest nodes to the current hash, while Quorum B are the

Diagram 4: Procedure to activate a masternode.

Masternode network performance maintenance

In theory, malicious actors could also run ION masternodes, but not provide any of the quality service that is required of the rest of the network. To reduce this possibility and discourage people from using the system to their advantage, all nodes must regularly ping the rest of the ION masternode network to ensure they remain active. This work is done through a selection of 2 quorums per block. At every new block hash, Quorum A checks the service of Quorum B. Quorum A are the closest nodes to the current hash, while Quorum B are the furthest nodes from said hash.

Masternode A (1) checks Masternode B (rank 2300)

Masternode A (2) checks Masternode B (rank 2299)

Masternode A (3) checks Masternode B (rank 2298)

The masternode network is self-monitoring. Approximately 1% of the network will be checked for each block added to the blockchain. This results in the entire masternode network being checked approximately six times per day. To maintain this trustless system, nodes are selected randomly via the quorum system; the network also requires a minimum of six violations in order to deactivate a node (Duffield and Diaz, 2015).

Coin development roadmap

ionomy.com will foster development on the open source core code for ION by defining targets, posting specifications for bounties, and paying independent developers for completed and validated commits. This approach allows the ionomy core development team to focus on what they do best, building the mobile and social games at the heart of the ION economy. The bounties engage the best talent from the developer community to enhance the core coin code while decentralizing coin development. The ION community can collectively influence the direction of the coin: if the community wants a feature and is prepared to post a bounty, the bounty will motivate developers to build it.

Payments for the bounties will be held in multisignature wallets. Pull requests are first implemented in the test network environment. Once deemed to meet the requirements and specifications set forth in the bounty, pull requests will be merged into the main branch of ION source code on github and bounties will be paid directly to the code developer.

Bounties

The following bounties have been identified as post launch priorities:

- Time delay transaction / Safe address (see example #1 below for further specification)
- Smart contract / escrow
- Colored coins / side chains / assets (see, for instance, example #2 below)
- HTML5 wallet
- Electrum wallet
- ION-j for mobile wallet based on java
- In-wallet social integration

Bounty example #1: Time delayed transactions with safe address*

The problem: Cold wallets — storage addresses with completely privately generated keys holding coins that are never online — provide the best known security in cryptocurrency. Users can print a private key on paper wallet that can be stored in a safe location. The optimal network, however, depends upon widespread participation by users holding ION in online wallets. Consider this scenario: If user Jane had a connected wallet (or masternode) at work and she leaves it running at night, then Dick, an employee in the IT department, could hack into her computer and send all her coins to his own address. Jane would have no remedy.

The bounty: Create a safe address system with delayed transactions to protect the ION owner even if the private key security is compromised. The developer will create an on-chain parameter that sets a variable delay in any send action for a given address, and points the wallet contents to a designated failover address if triggered. Now if Jane sets the time delay parameter to 10,000 blocks, then when Dick hacks her wallet, Jane still has a week to trigger the failsafe. If she does not trigger the failsafe, Dick gets her coins. But if she catches the attack in time, she can simply send a signal which diverts the coins to her cold wallet address. From there she can delete the compromised keys, and start fresh with new security measures, access her safe wallet and start staking again. The developer who wins the bounty will provide ION users with a whole new level of security: a "warm" wallet which strikes a balance between the safety of a cold wallet and the utility of a hot wallet. The "stake safe" system will optimize speed and security for the network and reward opportunities for the individual.

**This bounty example is a simplification for illustrative purposes. Actual bounties, posted on github, will fully detail specific requirements and parameters.*

Coins in context

Historically, most cryptocurrencies are designed to incentivize miners and stakers to expand and secure the network. Since low-difficulty mining is highly profitable, this brings some attention to the coin and begins to distribute it. However, these users are quick to divest their holdings without an ongoing driver of value. As coin supply rises faster than adoption growth, supply overwhelms demand, reducing the coin's value. While the coin may have expanded more distributed, it is still concentrated among a small community of investors and

Coins in context

Historically, most cryptocurrencies are designed to incentivize miners and stakers to expand and secure the network. Since low-difficulty mining is highly profitable, this brings some attention to the coin and begins to distribute it. However, these users are quick to divest their holdings without an ongoing driver of value. As coin supply rises faster than adoption growth, supply overwhelms demand, reducing the coin's value. While the coin may now be somewhat more distributed, it is still concentrated among a small community of core users and transient holders whose primary interest is financial gain. Speculators and traders may buy the coin, but they are also short term holders. The cycle of price manipulation and massive sell offs repeats and the result over time is a devalued coin with low visibility, poor reputation, and a user base comprised of transient profiteers with no interest in a long term investment.

By contrast, the relationship between ionomy.com and ION is designed to build value from the start. ionomy.com produces and sells digital goods with a focus on mobile and social gaming applications. The company funds a system of social and financial incentives to cultivate an engaged user base. Users are rewarded for activity within the company's products. By continuously creating desirable uses for ION, the company incentivizes more users to join the ecosystem. The user base then consumes more IONs, creating demand and scarcity.

At the same time, masternodes reward users for holding ION and performing work to secure the integrity of the network and blockchain. Furthermore, ION features powerful technical capacities designed to attract entrepreneurs to build new businesses, expand the user base, and increase the utility of the coin.

Conclusions

ION integrates static proof of stake (PoS v.3) system with an incentivized masternode/wallet matrix. The result is fast transaction confirmation, reliable network security, enhanced privacy through decentralized coin mixing, and reduced price volatility. This technological foundation establishes possibilities for smart contracts, colored coins, side chains and advanced security mechanisms.

This combination of ION's powerful coin technology with ionomy.com's creative corporate plan brings about compelling opportunities. Entrepreneurs and developers can leverage a social network of engaged customers and investors in a way that never before has been attempted in this industry.

Acknowledgements

Special thanks to contributing editors including:

Robert Hoppenfeld, Derek Broyhill and James Pass

References:

Blockchain.info. (2012). *Bitcoin Median Transaction Confirmation Time (With Fee Only)*. Retrieved from <https://blockchain.info/fr/charts/avg-confirmation-time>

Duffield, E. (2015). *Dash: Video Series - #4 - Incentivized Infrastructure and Masternodes. *DVS15E04. Retrieved March 28, 2016, from <https://www.youtube.com/watch?v=FY1mciGGhO4>.

Duffield, E. and Diaz, D. (2015). *Dash: A Privacy-Centric Crypto-Currency*. Retrieved from: <https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf>.

Duffield, E., Schinzel, H., and Gutierrez, F. (2014). *Transaction locking and masternode consensus: A mechanism for mitigating double spending attacks*. Version 2. Retrieved from <https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf>

Gautham. (2016). *Blockchain Monday Blues Due to Spam Transactions on Bitcoin Network*. NEWSBTC. Retrieved from: <http://www.newsbtc.com/2016/03/02/bitcoin-network-spam-attack/>

Appendix A

Sample ION block

```
SetBestChain: new best=0254614e1a37e7d1681738031a1ea18efa53773972b1b6cedaefb1a4877d926c height=5043
trust=23477951177320352418
blocktrust=1099304894429909
date=04/05/16 21:52:00
ProcessBlock: ACCEPTED
connected to self at 25.12.221.127:39286,
Successfully synced, asking for Masternode list and payment list

IONd masternode list
{
```



```
date=04/05/16 21:52:00
ProcessBlock: ACCEPTED
connected to self at 25.12.221.127:39286,
Successfully synced, asking for Masternode list and payment list

IONd masternode list
{
  "25.12.221.127:9999" : 0
}

CommitTransaction:
CTransaction(hash=fff53d85c32a301bf61d6cde7951667e7740292e8f360c614aeb18eed7a143e8,
nTime=1459893428,
ver=1,
vin.size=1,
vout.size=2,
nLockTime=0)
CTxIn(COutPoint(50f90a5bc8, 1),
scriptSig=3045022100e135cbb17ee9fc)
CTxOut(nValue=1000.00,
scriptPubKey=OP_DUP OP_HASH160 dd28713d7c72c6a6017a98dd8f29743cf4ce6a49 OP_EQUALVERIFY OP_CHECKSIG)
CTxOut(nValue=8.03999,
scriptPubKey=OP_DUP OP_HASH160 7b9a6410aea5fd21755d42778b65b5db5c898b36 OP_EQUALVERIFY OP_CHECKSIG)
keypool keep 13
```
