Bata Cryptocurrency Whitepaper

Bitcoin Firewall 1.1

BATA.IO

Table of Contents

Table of Contents 2

Bitcoin Firewall (v 1.1) **3-4**
Abstract 3
Why a firewall? 3-4

>51% majority hash-power attack **4-6**
Technical overview 4
Proof of concept 5
Recent examples 6

Attacks on BATA (BTA) **6-9**
Pumping & Dumping 6
Network flooding 7-8
Double-spend @ Bittrex 8
Prevention & Mitigation 8-9

Real-time 'intelligent' hard-fork protection **9-11**
Research & developments 10
Proof of effectiveness 11

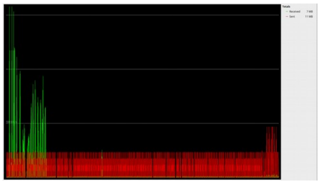
References **12-13**

Copyright: August 1, 2017 Justin Percy justinpercy@protonmail.com
Founder of Biznatch Enterprises & Profit Shares Platform, BATA developer.
Public Development Repository: https://github.com/BiznatchEnterprises/BitcoinFirewall

World's first implementation of connections firewall & artificially intelligent attack detection.

Why a firewall?

"Attackers chosen coins that are traded on big exchanges (in this case our friends from Bittrex) and made a double spend attack due to owning more than 51% hashes needed." [1]



Bitcoin Firewall 1.1 uses a very unique method for detecting potential hard-fork attacks, coupled with dynamic block chain DDoS flooding. All connected nodes/peers are examined using a dynamic rule set. By quickly avoiding long-term acceptance of malicious commands and transactions, Bitcoin based developers of crypto-coins can easily mitigates risks involved with low network hash-rates, and the costs involved with attempting to maintain the majority of network hashing.

If rule set criteria are met, the connecting node is further examined to verify that their blockchain start height is within safe limits of the average among all peers connected. Range-based dynamic blockchain checkpoints implementing averages instead of static heights, further enhance network security by limiting potential attacks known as "more than 51% of distributed hashing power". Once a potential attack is detected: the connected node/peer is forcefully terminated and added to a session blacklist and immediately refused future connections. This can be considered a temporary session break, for safety.

"Actually, it's very easy to do damage to the network once you have 51%; just build your own chain faster than the network, and broadcast it whenever you like. If you send some of your coins to a new address in your own chain, all the transactions issued in the live network by spending those same coins will be reversed at the moment the longer chain is broadcast." [2]

"An attacker that controls more than 50% of the network's computing power can, for the time that he is in control, exclude and modify the ordering of transactions. This allows him to: Reverse transactions that he sends while he's in control, Prevent some or all transactions from gaining any confirmations, Prevent some or all other generators from getting any generation, The attacker can't: Reverse other people's transactions, Prevent transactions from being sent at all (they'll show as 0/unconfirmed), Change the number of coins generated per block, Create coins out of thin air, Send coins that never belonged to him." [3]

“Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. However, if a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy. One approach to preventing these “Sybil attacks” is to have a trusted agency certify identities. This paper shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.” [4]

>51% majority hash-power attack

Mining new coins requires consensus among all nodes on the network to agree upon validation of new blocks containing existing (spent) confirmed transactions. Mining pools compute new hash values and send the data to the network via the nodes, eventually showing up in a client wallet. This process is very complex and requires all peers to cooperate by confirming and transferring funds safely among all participants of the network efficiently.

Attackers are modifying open source wallets with sophisticated changes. These can alter the performance of ALL nodes and peers, and thus the consensus among them as well. This could become detrimental enough, similar to a distributed denial of service attack; Possibly for a short period of time, enough to lower the security of all nodes and peers and successfully by-pass all check-sum algorithms for spending confirmed funds twice.

“The client accepts the 'longest' chain of blocks as valid. The 'length' of the entire block chain refers to the chain with the most combined difficulty, not the one with the most blocks. This prevents someone from forking the chain and creating a large number of low-difficulty blocks, and having it accepted by the network as 'longest'.” [2]

Technical overview

"Until 2009, Finney's system was the only RPOW system to have been implemented; it never saw economically significant use. In 2009, the bitcoin network went online. Bitcoin is a proof-of-work cryptocurrency that, like Finney's RPOW, is also based on the Hashcash POW. But in bitcoin double-spend protection is provided by a decentralized P2P protocol for tracking transfers of coins, rather than the hardware trusted computing function used by RPOW. Bitcoin has better trustworthiness because it is protected by computation; RPOW is protected by the private keys stored in the TPM hardware… Bitcoins are "mined" using the Hashcash proof-of-work function by individual nodes and verified by the decentralized P2P bitcoin network." [3]

“Double-spending is an error in a digital cash scheme in which the same single digital token is spent twice or more. This is possible because a digital token consists of a digital file that can be duplicated or falsified. As with counterfeit money, such double-spending leads to inflation by creating a new amount of fraudulent currency that did not previously exist. This devalues the currency relative to other monetary units, and diminishes user trust as well as the circulation and retention of the currency. Fundamental cryptographic techniques to prevent double-spending while preserving anonymity in a transaction are blind signatures and particularly in offline systems, secret splitting.” [5]

“Bitcoin requires that all transactions, without exception, be included in a shared public transaction log known as a "block chain." This mechanism ensures that the party spending the bitcoins really owns them, and also prevents double-counting and other fraud. The block chain of verified transactions is built up over time as more and more transactions are added to it. Bitcoin transactions take some time to verify because the process involves intensive number-crunching and complex algorithms that take up a great deal of computing power. It is, therefore, exceedingly difficult to duplicate or falsify the block chain because of the immense amount of computing power that would be required to do so.” [6]

Proof of concept

Bitcoin, Litecoin and several other crypto-coins are less vulnerable to double spend attacks. The simple reason is: They have many decentralized mining pools, coupled with a very large amount of processing power. In monetary value: not worth attempting double spend attacks.

“It's much more difficult to change historical blocks, and it becomes exponentially more difficult the further back you go. As above, changing historical blocks only allows you to exclude and change the ordering of transactions. It's impossible to change blocks created before the last checkpoint. Since this attack doesn't permit all that much power over the network, it is expected that no one will attempt it. A profit-seeking person will always gain more by just following the rules, and even someone trying to destroy the system will probably find other attacks more attractive. However, if this attack is successfully executed, it will be difficult or impossible to "untangle" the mess created — any changes the attacker makes might become permanent.” [2]

"Hackers have tried to get around the Bitcoin verification system by using methods such as out-computing the block chain security mechanism, or using a double-spending technique that involves sending a fraudulent transaction log to a seller and another to the rest of the Bitcoin network. These ploys have met with only limited success.” [7]

“We have derived the probability for a successful double-spend, and tabulated it in various ways. We have also briefly discussed the conditions in which a double-spending attack can be economical, and hence likely.” [8]

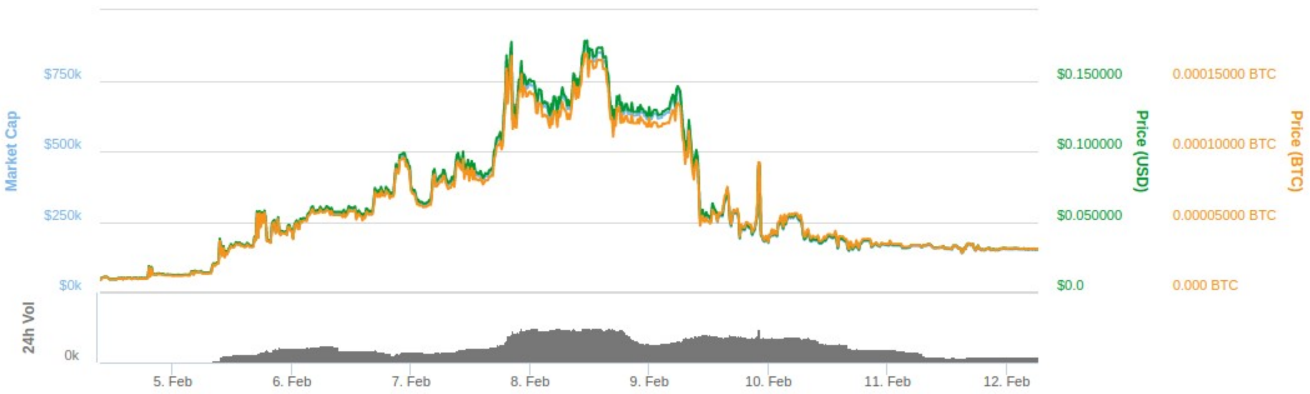
“Small-cap” coins are very vulnerable and highly susceptible to attacks if they only verify blocks using a Proof of Work algorithms. Recently exploited hashing algorithms such as SHA256, Scrypt, X11 and others have left many developers scrambling for solutions. Struggling with development funds, they have very few miners, and even less pools to contribute to the network processing power. Very low cost attacks can be simply rented by cloud services for short periods of time ensure the double-spend attack is successful… and they sometimes are very profitable!

Recent examples of double-spend attacks:

1) EMC2 Einsteinium [10]
2) QTL [11]
3) CANN [12]
4) BATA [12]
5) WBB [12]
6) UNB [12]
7) WUE [13]

Attacks on BATA (BTA)

Pumping & dumping



February 10, 2017 - “I am not a fan of Pump n Dumps, and I really hope this was not a plan by someone to target Bata for a PnD as this project has merits. But with Bittrex showing a 24 hr volume of 64+ BTC why are people selling at a loss? Don't panic and hold your price is what I would be thinking... But I am not expert in manipulating markets.” [15]

February 09, 2017 - "After a mega pump and dump afterwards and the big news was today can't see any news only riddles and that's what investors don't like m8" [16]

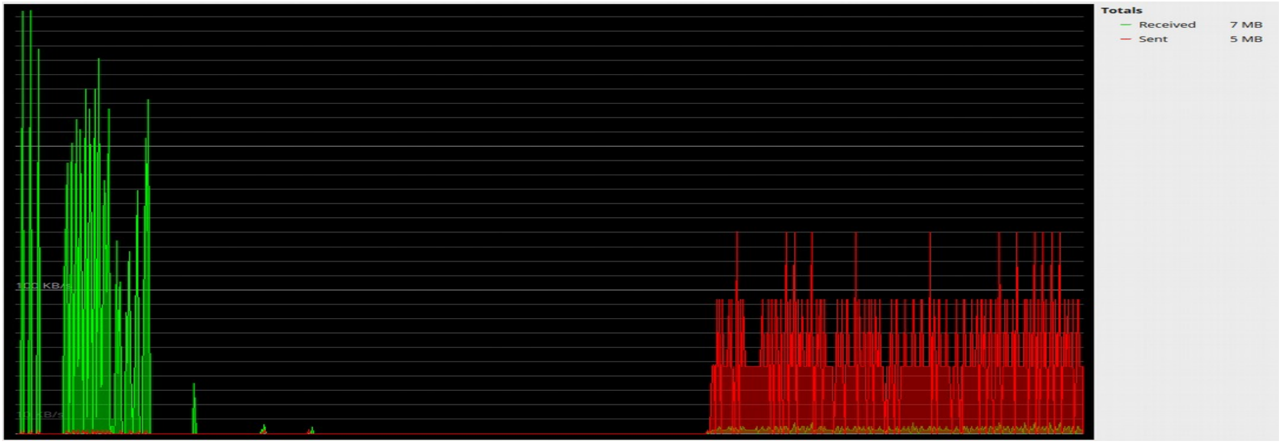
February 09, 2017 - "I must say I am very disappointed to see all these people come out of nowhere and suddenly accuse me personally of doing something." [17]

April 13, 2017 - "Get your facts straight before making accusations. There was no premine and nothing has been dumped. I have mined or bought all my BTA. Worst of all your comments are libelous… Here is your proof that GEENSTIJL is a pumper:" [18]

March 03, 2017 - "Speaking about the so-called speculative pumps, which, Yes, for weak projects was crucial and of course in such conditions it was like a holiday and of course it was death and speculation, but these projects were aimed at it and talk about some specially rigged solutions... I don't think, though... here, of course, speaking about the viability of the coin, we talk about all the instruments that can be applied to each phase " [19]

June 10, 2017, "Let's just ask ourselves, have these people really got anything better to do with their wretched, unrewarding lives? Is this really the best they can conjure up after days, months, and years of restlessness thinking about how to decredit someone else's work and success? If they spent more time evaluating their own lives maybe they'd actually get somewhere.." [20]

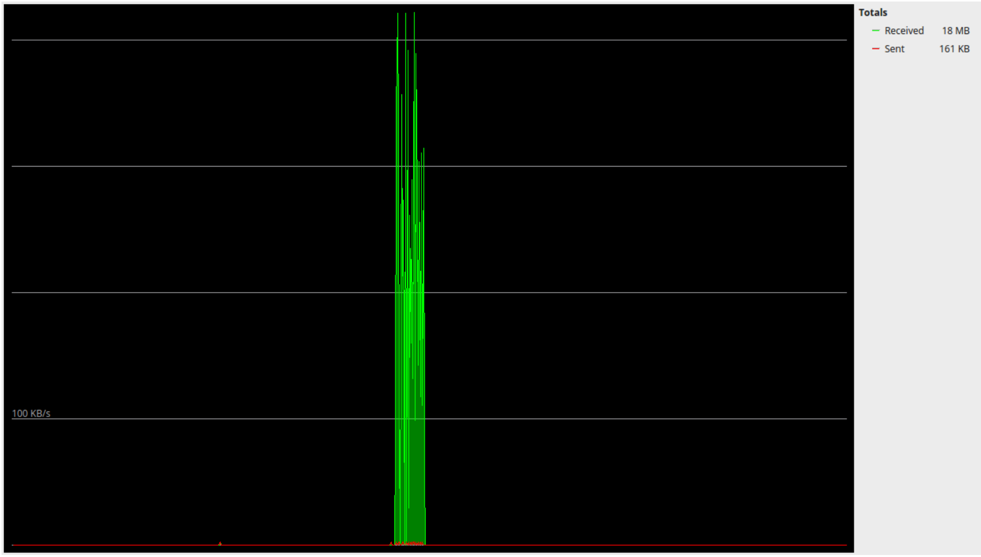
Network flooding



Modified wallets appeared to be tricking authentic versions to submit massive amounts of data throughout the P2P network, causing delays, increased orphan rates and overloaded nodes. By first initiating a submission of the attacking hard-fork transactions, the majority of distributed hashing power can be effectively reached as legitimate peers broadcasting the "real" block-chain database get knocked offline momentarily, opening up a window...

This brute force splitting of consensus, creates the necessary environment to achieve a full double-spend attack with success. Mining pools can be taken offline quite easily and thus the initial investment of achieving >51% hashing power can be greatly reduced.

Double-spend @ Bittrex successful (June, 2017)



Network hash-rates dropped below 3 GH, and attackers injected 79 BTA worth of double-spend transactions into Bittrex's wallet. This dual-attack was able to sell and withdraw the equivalent BTC before administrators at Bittrex discovered blockchain anomalies. Renting only 5 GH of Scrypt mining power costed approximately 0.044 Bitcoins for 5 hours. At these rental rates any attempts at double spending was a low risk / high reward scenario.

“A number of POW cryptocurrencies have attacked recently with a 51% attack. We were hit first time and lost a small number of BTA. Bittrex noticing put our wallet into maintenance mode, which we thank them for. We decided to lift the number of confirmations and put the wallet back online. More coins started to get attacked, with much higher confirmations, so Bittrex proactively put our wallet into maintenance before we were attacked again. For an attack to be worth the time and money, the reward must also be high. We since actively been monitoring the hashrate of each pool and maintaining our own pool with higher hash rates than any pool approaching the 50% mark...” [12]

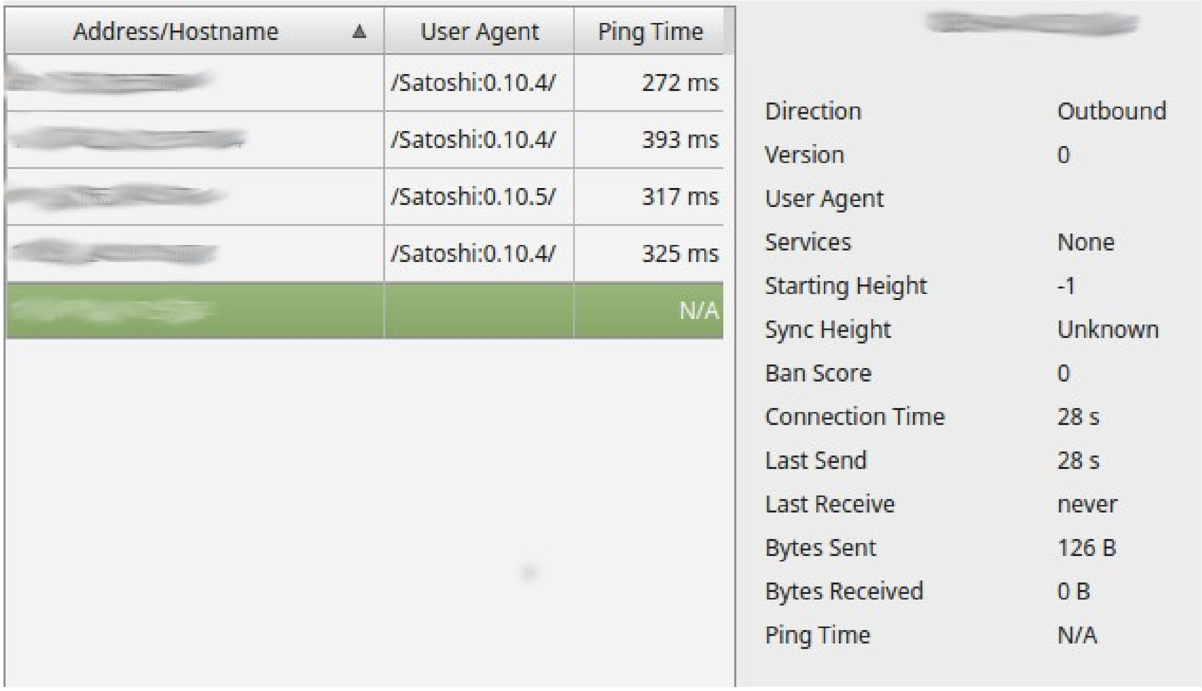
Prevention & mitigation

“Wallet maintenance implies one of several possible things could be happening: There could be a possible fork on the block chain. In order to protect funds, we have disabled the wallet until a consensus has been made on which chain is the proper chain. The wallet has been updated by the developer and the exchange is in the process of implementing the wallet update. The wallet daemon on our server has hung or crashed. The wallet is sending orphan transactions or having an issue that requires the developer to work with us on resolving.” [9]

“To perform a successful double-spending attack, the attacker A needs to trick the vendor V into accepting a transaction TRV that V will not be able to redeem subsequently. While this might be computationally challenging for A to achieve if TRV was confirmed in a Bitcoin block7, this task might be easier if the vendor accepts fast payments.” [14]

Real-time 'intelligent' hard-fork protection

A Bitcoin firewall has been a cliché concept very rarely discussed among developers. The controversial act of banning nodes and peers was manually time consuming and hard to distinguish good from bad network traffic automatically, in certain situations it has worked in slowing or eventually stopping an attack but can be very time consuming or fruitless if the attackers use a large-botnet with various ISPs, proxies or VPN/VPS connections.



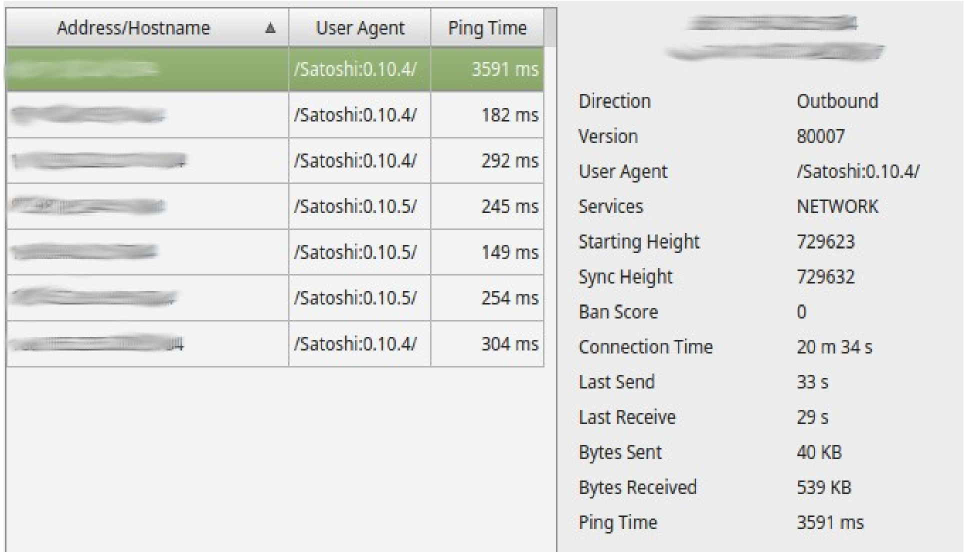
Address/Hostname ▲	User Agent	Ping Time
[redacted]	/Satoshi:0.10.4/	272 ms
[redacted]	/Satoshi:0.10.4/	393 ms
[redacted]	/Satoshi:0.10.5/	317 ms
[redacted]	/Satoshi:0.10.4/	325 ms
[redacted]		N/A

[redacted]

Direction	Outbound
Version	0
User Agent	
Services	None
Starting Height	-1
Sync Height	Unknown
Ban Score	0
Connection Time	28 s
Last Send	28 s
Last Receive	never
Bytes Sent	126 B
Bytes Received	0 B
Ping Time	N/A

Research & developments

Here is an example of valid BATA seed node connection stats after catching up on the block-chain sync after a few days.

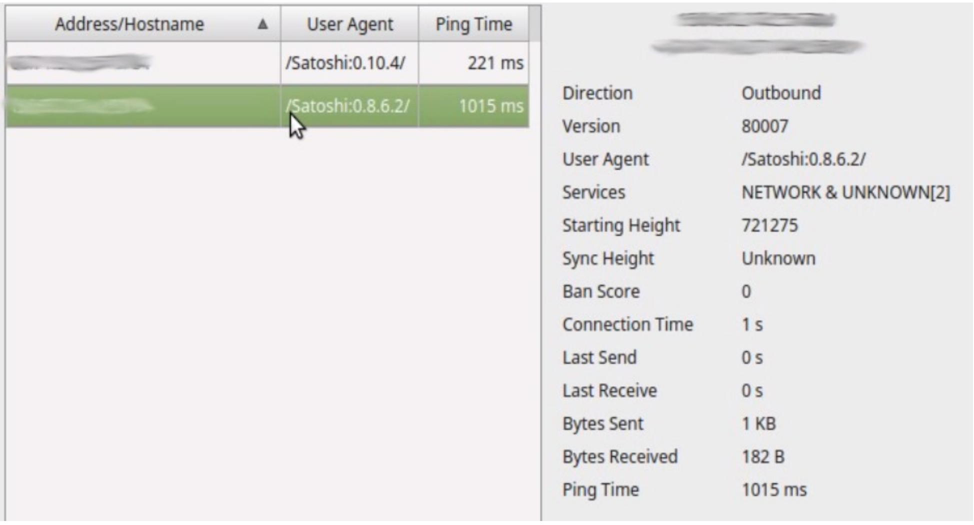


Address/Hostname ▲	User Agent	Ping Time
[redacted]	/Satoshi:0.10.4/	3591 ms
[redacted]	/Satoshi:0.10.4/	182 ms
[redacted]	/Satoshi:0.10.4/	292 ms
[redacted]	/Satoshi:0.10.5/	245 ms
[redacted]	/Satoshi:0.10.5/	149 ms
[redacted]	/Satoshi:0.10.5/	254 ms
[redacted]	/Satoshi:0.10.4/	304 ms

[redacted]

Direction	Outbound
Version	80007
User Agent	/Satoshi:0.10.4/
Services	NETWORK
Starting Height	729623
Sync Height	729632
Ban Score	0
Connection Time	20 m 34 s
Last Send	33 s
Last Receive	29 s
Bytes Sent	40 KB
Bytes Received	539 KB
Ping Time	3591 ms

Below is an example of a malicious peer attempting to avoid detection while sending double-spend transactions. What's important to focus on is the Starting Height comparisons above.

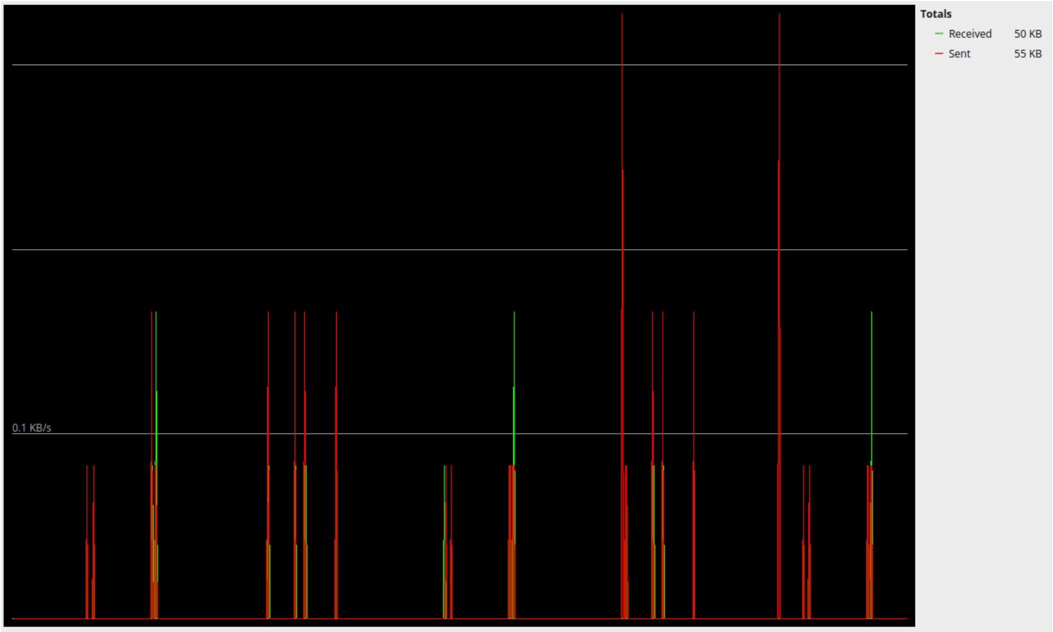


Address/Hostname ▲	User Agent	Ping Time
[redacted]	/Satoshi:0.10.4/	221 ms
[redacted]	/Satoshi:0.8.6.2/	1015 ms

[redacted]

Direction	Outbound
Version	80007
User Agent	/Satoshi:0.8.6.2/
Services	NETWORK & UNKNOWN[2]
Starting Height	721275
Sync Height	Unknown
Ban Score	0
Connection Time	1 s
Last Send	0 s
Last Receive	0 s
Bytes Sent	1 KB
Bytes Received	182 B
Ping Time	1015 ms

Proof of effectiveness



BATA core 10.5 - Debug.log output (edited):

```
2017-07-31 05:39:32 receive version message” NULL, version 0, blocks=-1, peer=2
2017-07-31 05:39:32 Added time data, samples 3, offset +1 (+0 minutes)
2017-07-31 05:39:34 Firewall - Netflood Detected: ***.***.***.***:5784
2017-07-31 05:39:34 Firewall - Blacklisted: ***.***.***.***:5784
2017-07-31 05:39:34 Firewall - Panic Disconnect: ***.***.***.***:5784
```

```
2017-07-31 05:47:29 receive version message: /Satoshi:0.8.6.2/: version 80007, blocks=718973
2017-07-31 05:47:31 Firewall - Netflood Detected: ***.***.***.***:5784
2017-07-31 05:47:31 Firewall - Blacklisted: ***.***.***.***:5784
2017-07-31 05:47:31 Firewall - Panic Disconnect: ***.***.***.***:5784
```

References:

[1] Double spend attack at Bittrex
https://steemit.com/bitcoin/@kingscrown/double-spend-attack-on-some-proof-of-work-coins-stopped-by-bittrex

[2] What can an attacker with 51% of hash power do?
https://bitcoin.stackexchange.com/a/662

[3] Bitcoin Weaknesses
https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

[4] The Sybil Attack
http://nakamotoinstitute.org/static/docs/the-sybil-attack.pdf

[5] Double-spending
https://en.wikipedia.org/wiki/Double-spending

[6] Proof of work system
https://en.wikipedia.org/wiki/Proof-of-work_system

[7] Breaking down Double Spending
http://www.investopedia.com/terms/d/doublespending.asp

[8] Analysis of hashrate-based double-spending
https://arxiv.org/pdf/1402.2009.pdf

[9] What does it mean when a wallet is in maintenance?
https://support.bittrex.com/hc/en-us/articles/115000233911-What-does-it-mean-when-a-wallet-is-in-maintenance-

[10] EMC2 Double spends
http://www.mediafire.com/file/ze49r1xevaoz0vt/EMC2+Double+Spends.pdf

[11] Doublesped almost 80,000 QuatlooCoin
https://steemit.com/cryptocurrency/@fyrstikken/major-fuckup-successful-double-spend-was-done-in-quatloocoin-on-bittrex-coin-to-be-delisted

[12] BTA Double spend @ Bittrex
https://bitcointalk.org/index.php?topic=1040956.msg19459031#msg19459031

[13] Hash attacks, fork and our instant & continued response
http://forum.mymue.com/topic/27/hash-attacks-fork-and-our-instant-continued-response/3

[14] Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin | https://eprint.iacr.org/2012/248.pdf

[15] Bitcoin Talk Forum - https://bitcointalk.org/index.php?topic=1040956.msg17797674#msg17797674

[16] https://bitcointalk.org/index.php?topic=1040956.msg17789916#msg17789916

[17] https://bitcointalk.org/index.php?topic=1040956.msg17790129#msg17790129

[18] https://bitcointalk.org/index.php?topic=1040956.msg18569997#msg18569997

[19] Bitcoin Talk Forum https://bitcointalk.org/index.php?topic=1040956.msg18052544#msg18052544

[20] https://bitcointalk.org/index.php?topic=1040956.msg19473240#msg19473240