

Welcome, **Guest**. Please login or register.

Forever

Login with username, password and session length

**News:** Latest stable version of Bitcoin Core: [0.11.2](#) [Torrent]

[HOME](#) [HELP](#) [SEARCH](#) [DONATE](#) [LOGIN](#) [REGISTER](#)

Bitcoin Forum > Bitcoin > Development & Technical Discussion (Moderator: gmaxwell) > **Possible way to make a very profitable 50 plus ish attack for pools?**

« previous topic next topic »

Pages: [1]

[print](#)

Author Topic: Possible way to make a very profitable 50 plus ish attack for pools? (Read 6705 times)

**Grinder**

Legendary

Activity: 1217



[Ignore](#)

**Possible way to make a very profitable 50 plus ish attack for pools?**

September 12, 2011, 07:18:36 PM

#1

I have searched the forum and Google, but I not find a discussion of this particular variation.

Say one pool starts paying 150% reward to attract more than 50% of the miners. At the next difficulty change block it mines until it solves it, and sets difficulty to 25%. Then it can mine on this chain and solve 4x as many blocks as everybody else, and still have the most difficult block chain. Is there any way to stop this, other than hoping that miners don't join?

**NO BITCOIN? NO PROBLEM! GET \$6,888 FREE BONUS!**

**BetCoin™**

Advertised sites are not endorsed by the Bitcoin Forum. They may be unsafe, untrustworthy, or illegal in your jurisdiction. [Advertise here.](#)

**Stephen Gornick**

Legendary

Activity: 1708



[Ignore](#)

**Re: Possible way to make a very profitable 50 plus ish attack for pools?**

September 12, 2011, 08:26:42 PM

#2

**Quote from: Grinder on September 12, 2011, 07:18:36 PM**

until it solves it, and sets difficulty to 25%

The difficulty is set by an algorithm and not something set by the miner. The miner could try changing the rules re: difficulty (i.e., and mine a blockchain that forks) but other clients wouldn't accept blocks as those blocks violate the Bitcoin protocol.

My OTC WoT Trust

**Sekioh**

Full Member

Activity: 163



FirstBits: 1sekioh



[Ignore](#)

**Re: Possible way to make a very profitable 50 plus ish attack for pools?**

September 12, 2011, 09:02:28 PM

#3

**Quote from: Stephen Gornick on September 12, 2011, 08:26:42 PM**

**Quote from: Grinder on September 12, 2011, 07:18:36 PM**

until it solves it, and sets difficulty to 25%

The difficulty is set by an algorithm and not something set by the miner. The miner could try changing the rules re: difficulty (i.e., and mine a blockchain that forks) but other clients wouldn't accept blocks as those blocks violate the Bitcoin protocol.

But this isn't quite true, as seen on the Geist coin and possibly soon the Namecoin, there's an attack that all other 49% accept the new forking of the chain as the original, and the 51% attacker can set accepts/declines at will. They 'mined' 20000 blocks in a hour instead of the previous 20000 taking days. 'violating' the protocol is only applicable to the few that are in the 49% and try to change rules, whoever has more than half makes the rules it seems from what I gather based on these attacks.

**theymos**

Administrator  
 Legendary



**Re: Possible way to make a very profitable 50 plus ish attack for pools?**

September 12, 2011, 09:11:17 PM

#4

**Quote from: Sekioh on September 12, 2011, 09:02:28 PM**

whoever has more than half makes the rules it seems from what I gather based on these attacks.

Activity: 2142

The majority can't change the rules used by the minority. The minority will always reject invalid blocks, even if the minority is just one person.



1NXYoJ5xU91Jp83XFVMHwwTUyZFK64BoAD

**im3w11**  
Sr. Member

**Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 12, 2011, 09:20:20 PM

#5

His coins will not be worth very much then...

Activity: 280



Ignore

**ArtForz**  
Sr. Member

**Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 12, 2011, 09:39:28 PM

#6

Activity: 406

Erm, no, those blocks are *\*valid\**.  
By exploiting the fact that retargeting ignores one block interval every period, it's possible for an attackers' fork chain to "jump backwards in time" and create lots of blocks at low difficulty without running nTime off into the far future.



Ignore

Bitcoin (and most *\*coin\**) rules re. block timestamps:  
nTime has to be > median of prev 11 blocks.  
nTime has to be < now() + some buffer.

let's say we have a chain with 4-block interval and 10 sec/block.  
Official chain, current diff for hashrate, blocks found at nominal time:

Code:

blk#	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
time	0	10	20	30	40	50	60	70	80	90	100	110	120	130	140	150

Now here's the weird part, we retarget after blocks 3, 7, 11, 15, and for block 3 we use 0 as first and 3 as last, for 7 we use 4 as first and 7 as last, ...

so what happens if an attackers chain has blk timestamps like this:

Code:

blk#	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
time	0	1	2	30	4	5	6	70	8	9	10	110	12	13	14	150

?  
first period (#3 - #0) is 30s as before  
2nd period is (#7 - #4) ... 66s  
3rd period is (#11 - #8) ... 104s

Whoops.

Obviously this ignores the "problem" of the attackers chain having way lower sum-of-difficulty but thats easy to fix:

Code:

blk#	16	17	18	19	20	21	22	23	...
time	16	17	18	19	20	21	22	23	...

just keep driving diff up at maximum speed until you have the same total work as the real chain. result-> the attackers chain does not violate the block timestamp rules, finishes at a *\*earlier\** block timestamp than the real chain, ends up at a higher total work as the real chain, but contains way more blocks.

This was done on the GeistGeld chain yesterday/today, so it's not a theoretical problem.

bitcoin: 1Fb77Xq5ePFER8GtKRn2KDbDTVpJKfKmpz  
i0coin: jNdyvvd6v6gV3kVJLD7HsB5ZwHyHwAkfdw

**ByteCoin**  
Sr. Member

**Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 12, 2011, 10:06:23 PM

#7

Thanks for the clear explanation ArtForz!

Quote from: ArtForz on September 12, 2011, 09:39:28 PM

Now here's the weird part, we retarget after blocks 3, 7, 11, 15, and for block 3 we use 0 as first and 3 as last, for 7 we use 4 as first and 7 as last, ...

Activity: 416



Ignore

It's clear that the calculation needs to be made piecewise continuous, so for 7 we use 3 as the first.


Quote from: ArtForz on September 12, 2011, 09:39:28 PM

Obviously this ignores the "problem" of the attackers chain having way lower sum-of-difficulty but that's easy to fix - just keep driving diff up at maximum speed until you have the same total work as the real chain.

Here's where I get confused. I haven't looked at the calculation in detail but surely you can't get the same total work as the real chain without doing approximately the same amount of hashing as the

real chain, no matter how many blocks is in your chain or how you've manipulated the difficulty?  
Please explain further...

ByteCoin

**ArtForz**  
Sr. Member  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 12, 2011, 10:10:58 PM

#8

Activity: 406




Ignore

No, obviously you need to do the same or more total hashes as the real chain (it is a 51% attack...)  
The "bad" part is that you can make your chain have more blocks while having the same start and end nTime.

And yes, it \*should\* be using 3-7, 7-11, ... but it doesn't. (probably to avoid the issue of the first interval after genesis, as you'd need to know when hashing of genesis started = the timestamp of the block before genesis).

The code I'm currently playing with gets around this by special-casing that first retarget to have a nInterval-1 span instead of nInterval.

bitcoin: 1Fb77Xq5ePFER8GtKRn2KDbDTVpJKfKmpz  
i0coin: jNdyvvd6v6gV3kVJLD7HsB5ZwHyHwAkfdw

**ArtForz**  
Sr. Member  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 12, 2011, 10:17:13 PM

#9


Activity: 406



Ignore

Oh, and this also means this isn't a too massive issue for bitcoin simply due to the scale and time required (attacker needs more hashrate than the real net over at least 4-5 real retargeting periods for it to be somewhat effective, more time = more profit), but it could be pretty bad news for altchains.

bitcoin: 1Fb77Xq5ePFER8GtKRn2KDbDTVpJKfKmpz  
i0coin: jNdyvvd6v6gV3kVJLD7HsB5ZwHyHwAkfdw

**ByteCoin**  
Sr. Member  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 12, 2011, 10:48:48 PM

#10

Activity: 416



Ignore

Quote from: ArtForz on September 12, 2011, 10:10:58 PM


No, obviously you need to do the same or more total hashes as the real chain (it is a 51% attack...)  
The "bad" part is that you can make your chain have more blocks while having the same start and end nTime.

Ok so it's a 51% attack which replaces the whole block chain.

You seem to be implying that the main negative effect is that the attacker gets more blocks over the period than he "deserves" from his hashing power. However, isn't the main effect that all the previous coinbase transactions are deleted and hence all transactions are declared invalid? This would effectively destroy the system and the response would be to either lock in the valid chain (preventing the attack) or start again with a new genesis block. Either solution would result in the attacker having wasted his hashing power.

Is this purely a destructive attack or can it be made profitable?

ByteCoin

**ArtForz**  
Sr. Member  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 12, 2011, 10:59:16 PM

#11

Activity: 406



Ignore

Depends, obviously this one is destructive, but there's a few variations on it.

A "fun" one that doesn't require orphaning massive parts of the chain:


With decently > 50%, only fork the chain if legit miners find > 5 blocks in a row (as that'd reset the median to where it should be) or the last block in a diff period (as that would prevent the wanted diff drop).

Broadcast blocks as usual.

Result: while things go mostly as normal (well, with quicker blocks the network now has over twice the hashpower and a few shortish chain forks getting orphaned), nTime of the chain except for the last block in each period basically stops increasing, and difficulty starts dropping after 2-3 retargeting periods.

So basically "a majority of miner hashpower can decide to near-arbitrarily lower difficulty, and there's nothing short of a chain lockin or changing the retarget rules to stop em"

bitcoin: 1Fb77Xq5ePFER8GtKRn2KDbDTVpJKfKmpz  
i0coin: jNdyvvd6v6gV3kVJLD7HsB5ZwHyHwAkfdw

**ArtForz**  
Sr. Member  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 12, 2011, 11:08:32 PM

#12

Activity: 406



another variant, which doesn't orphan anything:

get a \*massive\* majority of miners to switch to nTime rules like this for mining:

```
if ((pPrevBlock->nHeight+2) % retarget_block_count == 0)
```

```
    set nTime as normal
```


```
else
```


```
    block->nTime = medianofprev11()+1
```

Ignore

Once enough miners switch to this so that "legit miners finding 6 blocks in a row" gets unlikely enough so it doesn't occur over 2+ diff periods, difficulty starts decreasing. Adding some limits to make it head towards any arbitrary difficulty instead of going for "maximum decrease" is pretty simple.

bitcoin: 1Fb77Xq5ePFER8GtKRn2KDbDTVpJKfKmpz  
i0coin: jNdvyyvd6v6gV3kVJLD7HsB5ZwHyHwAkfdw

**makomk**  
Hero Member  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 13, 2011, 01:17:34 PM

#13

Quote from: ArtForz on September 12, 2011, 10:10:58 PM

The code I'm currently playing with gets around this by special-casing that first retarget to have a nInterval-1 span instead of nInterval.

Activity: 686


Presumably if the Bitcoin developers decided they needed to change the difficulty algorithm fix this issue, they could just as easily change over from nInterval-1 to nInterval at a specified block some time in the future?



Ignore

Quad XC6SLX150 Board: 860 MHash/s or so.

**SIGS ABOUT BUTTERFLY LABS ARE PAID ADS**

**ArtForz**  
Sr. Member  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 13, 2011, 04:29:22 PM

#14


Yes. Obviously you'd put a chain checkpoint right before the switchover to prevent any future 51% attack from mucking with earlier blocks.  
GeistGeld reloaded is the first chain testing retargeting over the full period, we'll see how that goes.

Activity: 406



Ignore

bitcoin: 1Fb77Xq5ePFER8GtKRn2KDbDTVpJKfKmpz  
i0coin: jNdvyyvd6v6gV3kVJLD7HsB5ZwHyHwAkfdw

**ctoon6**  
Sr. Member  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 16, 2011, 12:52:13 AM

#15

if somebody makes a block that does not fit in the rules of your client, it rejects it, simple as that. the rules your client has set can not be changed no matter how many bad blocks it rejects. the only thing an attack like that would do is waste yours and their time and their energy and money. sure they could make some transactions look like they never existed, but i don't see that going on for long, as it would cost large amounts of energy.

Activity: 350



we are at 13.8 Thash/s only to be predicted to grow. id imagine, in less than 60 days, it will be over 14Thash/s

thats about 18,000 6990s  
and i doubt you could even buy half that many. and at USD770 each, it would be USD13M, not counting the energy to run all that.




Ignore

or another scenario, you use cpus, since there several orders of magnitude more cpus than gpus, it would take like 650000 1100T's to get less than half of the hashing power.

overall, its not possible, you literally have to match or beat everything the ENTIRE network throws at you. it would be a never ending stream of spending money. although you do not need 50% to do damage, you could start doing damage at like 30% on an irregular basis.

Buy games & TF2 items with BTC  
Google+

**Grinder**  
Legendary  


 **Re: Possible way to make a very profitable 50 plus ish attack for pools?**  
September 16, 2011, 08:47:22 AM

#16

Quote from: ctoon6 on September 16, 2011, 12:52:13 AM

overall, its not possible, you literally have to match or beat everything the ENTIRE network throws at you. it would be a never ending stream of spending money. although you do not need 50% to do damage, you could start doing damage at like 30% on an irregular basis.

Activity: 1217



Ignore

What part of the word "pool" do you not understand? I'm not talking about beating the total hash rate of the network, but about enough miners colluding to maximize profits. For every miner that joins, the hash rate of the honest part will get smaller and easier to beat. I didn't get the technical part quite right, but ArtForz has already explained how it could be done.

Sponsored by Private Internet Access, a Bitcoin-accepting VPN.



Powered by SMF 1.1.19 | SMF © 2006-2009, Simple Machines

