IOTA slack, 14-15. June 2017

Winston [9:01 AM]
"I've been thinking about it for a little while. Essentially, to do an attack or hold the network hostage, you don't have to beat out the hashing power of the entire network, just the hashing power of the network actively using the Tangle at any given moment.

So, an actor with enough hashing power who wants to trigger this process can start pushing out higher weight transactions at some point when network load is low. The network will have no choice but to increase the weights of normal transactions, because if they don't, they give that actor the ability to attack the network.

The actor (especially if its a few powerful miners in on this together) could probably keep pulling off this same attack until the average own weights of the Tangle are so high that only heavyweight miners can partake in creating transactions."
https://www.reddit.com/r/Iota/comments/6fhaa6/iota_is_the_future/ (edited)

Come-from-Beyond [9:07 AM]
All transactions have own weight = 1 (edited)

Sunny Aggarwal [9:25 AM]
joined #tanglemath

Sunny Aggarwal [9:30 AM]
Hi all, just learned about this channel. Am going to have a good time reading through the history! I have a lot of questions to ask! (edited)

[9:33]
@come-from-beyond I'm the one who posted the comment that @winston quoted. All transactions have an own weight of 1? This is a massive departure from the whitepaper. Regardless, even if you can't create high weight transactions, you can just create many transactions and have them reference only each other as a clump and essentially achieve the same effect as high weight single transactions

Winston [9:35 AM]
Thanks for joining this channel @sunnya97 ! I look forward to keeping an eye on (& learning from) the ensuing discussions. I hope you're able to ask all of your questions from reddit in here. We can summon Dr. Popov during his waking hours to join the discussion (edited)

dylan [10:01 AM]
curious to see who can comment on this

Nur Azhar [10:16 AM]
joined #tanglemath

Come-from-Beyond [12:37 PM]
@sunnya97 not really _massive_, WP talks about limiting the own weight, in IOTA its upper bound is 1. Also note that WP is about Tangle while IOTA is an implementation of Tangle concept.

Sunny Aggarwal [12:41 PM]
@come-from-beyond Yeah, you're right. My bad. The whitepaper does say
>in practice, the weight may assume only values 3n, where n is positive integer and belongs to

some nonempty interval of acceptable values
After all, the set of possible n could just be {0} (edited)

[12:42]
But okay, what about the case where you could just create the same effect with multiple transactions of weight 1?

Come-from-Beyond [12:43 PM]
Before or after the adaptation period of the transaction of interest is over?

Sunny Aggarwal [12:45 PM]
Before. As a way of messing with the tip selection process.

Come-from-Beyond [12:48 PM]
Merchants may refuse accept such transactions or if they accept them to get competitive advantage in speed of processing they will include possible fraud loss into their prices. It's like accepting 1-confirmation payment in Bitcoin.

Sunny Aggarwal [12:53 PM]
How would merchants be able to detect this? Also, my worry is less about double spends and more about powerful miners basically spamming the network (confirming only their own transactions, not randomly spamming) in order to outpace any transactions not created by them. That way anyone who wants a reasonable chance to not have their transaction left perpetually unconfirmed will have to get it processed by the miners. (edited)

Come-from-Beyond [12:55 PM]
> How would merchants be able to detect this?
This will likely be solved heuristically.

[12:55]
> Also, my worry is less about double spends and more about powerful miners basically spamming the network (confirming only their own transactions, not randomly spamming) in order to outpace any transactions not created by them. That way anyone who wants a reasonable chance to not have their transaction left perpetually unconfirmed will have to get it processed by the miners.
IOTA is for IoT where assumption of absence of an omnipresent adversary is pretty reasonable. (edited)

[12:56]
To continue we need to set some topology of economic clusters and apply your attack to it, otherwise it's near impossible to analyze, too generalized.

Sunny Aggarwal [12:58 PM]
If Iota is a _public_ ledger with a _publicly_ traded crypto asset with real value (one that happens to be #6 in terms of market cap) how can you assume no economically selfishly motivated actors?

Come-from-Beyond [12:58 PM]
It's pretty silly to assume that there will be NO economically selfishly motivated actors

[12:59]
I probably don't get what you mean

[12:59]

Are we talking about Tangle or IOTA?

[1:00]
Tangle is a spherical horse in vacuum. IOTA is Tangle implementation for IoT.

[1:00]
I can't analyze your attack for Tangle, too general.

[1:00]
Let's do it for IOTA.

Sunny Aggarwal [1:00 PM]
Sure, let’s do Iota specifically.

[1:01]
In Iota, you can’t stop someone from using the system for non-IoT purposes

Come-from-Beyond [1:01 PM]
right

Sunny Aggarwal [1:02 PM]
Here, let me try to approach this from a different angle

[1:03]
Iota’s system is fee-less if everyone does the PoW for their own transactions, right?

Fabio Federici [1:04 PM]
joined #tanglemath

Sunny Aggarwal [1:04 PM]
This means everyone is contributing computational power equivalent to their usage of the network. However, if everyone was able to do that, you could just do that on a blockchain as well and also achieve an effectively fee-less system.

[1:04]
In Bitcoin, if you made 10% of all transactions (paying 10% of all transaction fees), but also provided 10% of all hashing power, you’d also be the block winner for about 10% of the blocks. Amortized over time, this would roughly earn you 10% all of all transaction fees in the network, basically getting you to a net zero on transaction fee costs.

[1:05]
As this isn’t the case in Bitcoin where everyone provides equivalent hashing power to their usage of the network, I don’t see why it would magically be the case in Iota. Because there is a discrepancy in provided computational power and network usage, a PoW-computation market will emerge.

Come-from-Beyond [1:07 PM]
I suspect you assume infinite speed of transaction propagation. It's not true for nowadays Internet and very non-true for IoT meshnets.

[1:09]
If an adversary starts issuing a lot of transactions its neighbors will start sending them further, but because of latency this will go as a wave, not as a solid stream of transactions. Neighbors of the

immediate neighbors will work as a buffer, the next layer will buffer it too and so on until the wave is not smoothed completely.

[1:10]
You probably noticed that we don't use automatic peer discovery, one of the reasons is to keep IOTA network within security assumptions of IoT meshnets. (edited)

[1:10]
Manual neighbor tethering allows to prevent someone from becoming _omnipresent_.

Sunny Aggarwal [1:11 PM]
Oh hmmm, that's quite interesting

[1:12]
But what if someone just makes many nodes and disperses them all throughout the network so they all have different peers (edited)

Come-from-Beyond [1:12 PM]
This may lead to a successful censoring attack where others will be forced to do more PoW to get their transactions confirmed. (edited)

Sunny Aggarwal [1:14 PM]
Aha! Yes, this is what I was getting at. Someone (or a group of someones) with enough hashing power could do this to the point that they get the PoW to be hard enough that only they can do it (cause they have a disproportionate share of hashing power)

Come-from-Beyond [1:15 PM]
The same is applicable to Bitcoin, Ethereum and _all_ other PoW coins

[1:16]
Note that this attack is not cheap, so making it expensive is a solution. All attacks can be conducted, it's just the matter of budget.

Sunny Aggarwal [1:18 PM]
Well yes, the same _already_ happens in Bitcoin, Ethereum, and all other PoW coins. A few mining pools and people with dedicated hardware control such a disproportionate share of the hashing power that it's pretty much useless for anyone that's not in this small group to even partake in mining (which is why they don't)

Come-from-Beyond [1:19 PM]
Good for IOTA it's very hard to become _omnipresent_ in IoT and unlike those coins with block subsidy or fees there is no an incentive to conduct the attack during long period of time.

Sunny Aggarwal [1:21 PM]
I don't know enough about mesh network and IoT to be able to speak much about the omnipresence issue

[1:22]
But there are fees to be gained by charging them in return for your transaction instead of trying to outpace it

Come-from-Beyond [1:24 PM]

If you achieved omnipresence you can extort fees just for traffic passing thru your nodes)

[1:24]
No even need to generate more txs, just do censoring

Sunny Aggarwal [1:26 PM]
And the lack of a block subsidy actually makes things more problematic I think. In Iota, an attacker doesn't have to beat the hashing power of the rest of the network, just the hashing power of the network actively making transaction at a given point in time. Without the mining reward, there's no incentive for someone to be continuously be contributing to the security of the system (edited)

[1:27]
Ok, sure. Fine, not omnipresence. But enough nodes to be able to avoid being censored yourself.

unicornio [1:31 PM]
joined #tanglemath. Also, @pjeo joined.

Come-from-Beyond [1:34 PM]
block subsidy absence makes everything good in my opinion, it removes incentive to generate superwide tangle

[1:35]
You are right that you need to compete against active users only

[1:35]
50% of their hashpower to get 33% of total hashpower is enough

[1:37]
But it's a long-range attack which will be counteracted by means similar
to Bitcoin (checkpointing), Nxt (economic clusters), Ethereum (forgot what they use for that in the current version) (edited)

[1:37]
Again, you need to be omnipresent

[1:38]
otherwise you need more than 50%, can't say the order of magnitude because it heavily depends on network topology

[1:42]
(removed offtopic) (edited)

Gábor Lipovszki [2:01 PM]
joined #tanglemath. Also, @hazelnuts joined, @burkelibbey joined, @mylifecommander joined, @walling joined, @tedshield joined, @hopebloom joined, @guilou34 joined, @danhoooo joined along with some others.

m commander
[5:24 PM]
@come-from-beyond assuming there was a submesh designed by someone not with the montecarlo algo but according to some design plan, how can this not be an attack vector? especially as current

wallets give you no control about confirmations

[5:24]
i would love to have a wallet that gives me control about the # of confirmations but maybe also getting it confirmed from nodes within some `economic cluster` (not sure if that is the right word)

Come-from-Beyond [5:24 PM]
Explain how can it be used for an attack

m commander
[5:25 PM]
well assuming you are not implementing MC and are creating your own little net with malware nodes

[5:25]
as attach to tangle is random, some will attach to the net you control

[5:26]
some of these transactions may then require confirmations from nodes that you also control (not sure if I worded that correctly)

[5:26]
if the wallet works with only 1 confirmation, you could double spend i guess

f f [5:27 PM]
joined #tanglemath. Also, @razzlo joined.

Come-from-Beyond [5:28 PM]
For transactions with already passed adaptation period it doesn't matter what algo was used: RWMC, pure random or something else

curiousgypo [5:31 PM]
joined #tanglemath. Also, @masoholik joined, @xharann joined, @bigmambo joined.

m commander
[5:36 PM]
@come-from-beyond ok let me rephrase citing the whitepaper

[5:36]
It is important to observe
that we do not impose any rule for choosing the transactions to approve; rather,
we argue that if a large number of other nodes follow some “reference” rule (which
seems to be a reasonable assumption, especially in the context of IoT, where nodes
are specialized chips with pre-installed firmware)

[5:37]
what if the above were not true

[5:37]
and we had a lot of bad actors

Come-from-Beyond [5:37 PM]

then you can't make reasonable prediction on validity of transactions before the adaptation period is over

m commander
[5:37 PM]
that are connected with each other

Come-from-Beyond [5:37 PM]
this in turn means extended interval before confirmation

m commander
[5:37 PM]
ok where can I read up on the adaption period?

Come-from-Beyond [5:37 PM]
in the whitepaper

m commander
[5:37 PM]
ok let me read and get back

[5:37]
:slightly_smiling_face:

Come-from-Beyond [5:38 PM]
I'll be busy by that time, so don't expect swift response

m commander
[5:38 PM]
this is asynchronous

Jay Gatsby [5:39 PM]
joined #tanglemath. Also, @darknight1818 joined, @idsyours joined, @alegenoa joined, @limo joined.

Come-from-Beyond [7:12 PM]
@sunnya97 What timezone are you in? We were having nice chatting and then you disappeared in the middle of it. I hope I didn't make you bored.)

[7:12]
Ping me once you have time to continue, please

Paul H [7:27 PM]
http://s2.quickmeme.com/img/11/11e62c00359416b4d600250e6dd6d1daaa6bfd54ec6be7452482116eebf7b25e.jpg (81kB)

uvas [8:22 PM]
joined #tanglemath

m commander
[8:42 PM]

@come-from-beyond i had a quick look at the adaptation time and the parasite chain

[8:43]
@come-from-beyond and i dont`t understand it well enough to construct an attack yet :slightly_smiling_face:

[8:45]
@come-from-beyond it would be cool if the guy makes the videos makes an ELI5 animation for all the future adopters that only watch .GIFs on reddit

[8:46]
the guy that makes the other videos

[8:46]
animation about the double spending case

Winston [8:50 PM]
I've been considering it.
m commander
@come-from-beyond it would be cool if the guy makes the videos makes an ELI5 animation for all the future adopters that only watch .GIFs on reddit
Posted in #tanglemathYesterday at 8:45 PM
(edited)

Gue [8:52 PM]
joined #tanglemath

Sunny Aggarwal [8:57 PM]
@come-from-beyond Hey sorry! I'm on the East coast but accidentally pulled an all-nighter and crashed at 7:30 am. Just woke up. I'll get back to responding to this in a little bit. (edited)

Micah Zoltu [8:57 PM]
I believe the arguments @sunnya97 is making are all basically the same arguments I was making a few days ago.

Come-from-Beyond [8:58 PM]
great, we should throw a party here while everyone is here

uvas [8:58 PM]
woo woo

Micah Zoltu [8:58 PM]
Maybe @sunnya97 will be more interested than me in writing up a formal disproof. ¯_(□)_/¯

Come-from-Beyond [8:58 PM]
@micah.zoltu I was busy with exchange launch so didn't have time to read your posts

Micah Zoltu [8:58 PM]
I dropped the topic after it was made clear to me that my arguments wouldn't be heard without a formal disproof of the current system. :confused: (I don't have time for that) (edited)

Come-from-Beyond [8:59 PM]

hm, formal disproof is too boring, we might go just with common sense and use formal method only if we don't come to a consensus on some things

Serguei Popov [9:00 PM]
I'll join you in some hours, guys....

Micah Zoltu [9:00 PM]
https://iotatangle.slack.com/archives/C3V610ULS/p1496895149743937
Matthew Niemerg
You should formalize your argument.
Posted in #tanglemathJune 8th at 6:12 AM

Serguei Popov [9:00 PM]
(those students here make me nervous...)

Micah Zoltu [9:06 PM]
Up until that point, it seemed that the conclusion that was being arrived at is that Iota equilibrium requires the majority of participants behaving in a way that is "good for the network" rather than in a way that is purely selfish. I did not believe that there would be a large enough share of non-selfish individuals to prevent selfish individuals from taking over the network while it seemed like others believe that being selfish was likely too hard for most people to bother.

Tristan [9:07 PM]
:popcorn:

Micah Zoltu [9:08 PM]
My primary argument was that there exists a parent selection strategy that is as-good or better than the recommended parent selection strategy but hurts the network. Because there is no selfish incentive to use the recommended strategy over this strategy, over time participants will tend towards the competing strategy, which will continually degrade network health to the point where those participating in the selfish strategy can take over the network and change the _effective_ rules.

[9:09]
In particular, I believe the equilibrium is around large participants charging "transaction" fees to smaller participants for inclusion.

[9:10]
Thinking on it even more over the past few days, I'm concerned that this selfish strategy will actually reach the point where confirmation isn't possible because there are too many isolated sub-tangles that aren't merging regularly.

[9:10]
And an unconfirmed transaction is effectively worthless unless you implicitly trust the source to not double-spend.

Zachariah Drew [9:11 PM]
joined #tanglemath. Also, @tawarien joined.

Sunny Aggarwal [9:15 PM]
Yes. Precisely. @micah.zoltu's point is exactly what I was trying to get at as well. Those orphaned

subtangles will only be able to merge back into the main tangle by paying computationally powerful actors to confirm them. (edited)

Charles Jiang [9:16 PM]
joined #tanglemath. Also, @luxor joined.

projectShift (Ricardo)
[9:19 PM]
so, if I get the arguments right, you're both advocating that the holly grail for IOTA is to find a parenting method that is enforced by way of supporting selfish behaviors in such a way as to avoid sub-tangle isolation and convergent economic clustering around competitive approaches, so efficient that the vast majority of nodes will have it has near-optimal?

Jeff Schmidt [9:21 PM]
joined #tanglemath

Micah Zoltu [9:22 PM]
Dominant parent selection strategy, for the sake of attack defense, must be the most-selfish selection strategy.

[9:23]
The whitepaper has a number of attack defenses, but they all assume that the dominant parent selection strategy is the _recommended_ strategy. They do not assume that the dominant parent selection strategy is the most selfish strategy.

[9:23]
This, IMO, invalidates the attack defenses as described by the whitepaper.

Winston [9:24 PM]
Let CfB comment on the above. I think he was busy and not around the last time you brought this up. Love it (edited)

Micah Zoltu [9:24 PM]
Alternatively, you need a parent selection strategy that is enforced by the protocol, which I haven't been able to come up with for a tangle.

projectShift (Ricardo)
[9:26 PM]
@come-from-beyond chim in, mate. Open minded like you like it :slightly_smiling_face:

Micah Zoltu [9:26 PM]
I believe he indicated he had to step away.

projectShift (Ricardo)
[9:27 PM]
just a placeholder, so he knows where to take it from

Sunny Aggarwal [9:28 PM]
Furthermore, this is exacerbated by the fact that the selfish parent selection strategy doesn’t need to be dominant in the network overall. It just has to be dominant amongst active users of the network at any given moment.

qra qra [9:33 PM]
joined #tanglemath

Come-from-Beyond [9:35 PM]
just came home from dog walking

[9:35]
reading

spectro [9:36 PM]
joined #tanglemath

Come-from-Beyond [9:38 PM]
> Up until that point, it seemed that the conclusion that was being arrived at is that Iota equilibrium requires the majority of participants behaving in a way that is "good for the network" rather than in a way that is purely selfish. I did not believe that there would be a large enough share of non-selfish individuals to prevent selfish individuals from taking over
the network while it seemed like others believe that being selfish was likely too hard for most people to bother.
Simulations on a 20-cluster tangle where transactions were picked completely random showed that most of transactions were still confirmed. Do you have an example of such selfish strategy that leads to problems with confirmations?

Micah Zoltu [9:38 PM]
Random parent selection is good for the network, but not selfish.

Come-from-Beyond [9:39 PM]
Give me example of _selfish_ one.

Micah Zoltu [9:39 PM]
The selfish strategy I believe is to _never_ choose a parent that isn't something you personally care about.

[9:39]
There is no selfish incentive that I have seen to choose anything other than your own transaction as your parent.

Come-from-Beyond [9:40 PM]
What percentage of such active users do we need to create troubles?

Micah Zoltu [9:40 PM]
I don't believe it matters since I believe this strategy is _better_ (from a selfish perspective), over time everyone save for the altruistic participants will migrate towards it.

[9:41]
By selecting your own transactions as parents, you increase the chances that someone else will pick you as their parent using one of the random selection strategies.

Come-from-Beyond [9:41 PM]
We assume that 67% of nodes stick to one of the good strategies.

Micah Zoltu [9:41 PM]
:point_up: This is what I believe is _hugely_ dangerous.

[9:42]
That requires 67% of participants (by computing power) to _not_ be self interested and instead be altruistic participants to some degree.

Come-from-Beyond [9:42 PM]
--> nodes <--

Micah Zoltu [9:42 PM]
Computing power I think is more accurate, since one can simulate a node with computing power.

Come-from-Beyond [9:42 PM]
Are you familiar with concept of _network-bound_ PoW?

Micah Zoltu [9:43 PM]
And in fact I believe node simulation is _cheaper_ than actually running a real node as you can leverage shared resources across simulations. (edited)

Come-from-Beyond [9:43 PM]
not processor-bound, not memory-bound, but network-bound

Micah Zoltu [9:43 PM]
Network bandwidth can be bought just as easily as CPU/RAM.

Come-from-Beyond [9:44 PM]
This is a bold claim for IoT, are you familiar with LoRa?

Fahad Sheikh [9:44 PM]
just a suggestion. The discussion in Tanglemath should somehow be saved and posted in the forum. Because this is the very discussion that people want to read to see how technically sound the Tangle is. Or you should only do it in the forum :slightly_smiling_face:

Micah Zoltu [9:44 PM]
I can run a geo-located cluster in AWS to achieve both latency advantages (geo location) and bandwidth advantages (pay for bandwidth).

Come-from-Beyond [9:44 PM]
We are talking about IoT, don't forget that

Micah Zoltu [9:44 PM]
I think it is unsafe to assume that IoT devices dominate the network. There is no way to prevent non-IoT devices from participating in the network and simulating as many IoT devices as one has the computing resources to simulate.
Come-from-Beyond
This is a bold claim for IoT, are you familiar with LoRa?
Posted in #tanglemathYesterday at 9:44 PM

[9:45]

You are about the 5th person to suggest this. :slightly_smiling_face: I believe several people are doing periodic snapshots of it. @projectshift I know was for a bit...
Fahad Sheikh
just a suggestion. The discussion in Tanglemath should somehow be saved and posted in the forum. Because this is the very discussion that people want to read to see how technically sound the Tangle is. Or you should only do it in the forum :slightly_smiling_face:
Posted in #tanglemathYesterday at 9:44 PM

Come-from-Beyond [9:45 PM]
Well, I think that we should look at solutions like LoRa. The challenges they tackle clearly show that you are wrong. Or LoRa is far from the reality.

[9:46]
I believe the former is more probable than the latter because LoRa is backed by a lot of money

[9:46]
I mean A LOT of money

Micah Zoltu [9:46 PM]
I'm assuming by LoRa you are referring to this? https://en.wikipedia.org/wiki/LPWAN (edited)

Come-from-Beyond [9:47 PM]
How many KB can you transfer within 1 hour via such network over 1 km?

[9:47]
just a ballpark number

Micah Zoltu [9:47 PM]
If I understand you correctly, you are proposing a massive IoT mesh network backed by LoRa (or similar)?

[9:48]
And you are then operating under the assumption that such a network has massively constrained transfer capacity?

Come-from-Beyond [9:48 PM]
IoT environment is very constrained. Even basic things like RSA algos have to be replaced with much simpler algorithms. (edited)

Micah Zoltu [9:48 PM]
So either you have a single global mesh network, or eventually that mesh network needs to hop onto the internet to cross large distances.

[9:49]
A single global mesh network I think is unrealistic in the forseable future, there is just too much expanse of earth surface that isn't easily covered by a mesh network (e.g., Oceans).

Come-from-Beyond [9:49 PM]
If you check the convo above you will see "omnipresence" mentioned quite a lot of times

Micah Zoltu [9:50 PM]
Which means you have to piggyback on the internet for long-jumps, and as soon as you do that you

are susceptible to someone utilizing non-IoT resources (AWS nodes) to simulate millions or billions of IoT devices.

Come-from-Beyond [9:51 PM]
> A single global mesh network I think is unrealistic in the forseable future, there is just too much expanse of earth surface that isn't easily covered by a mesh network (e.g., Oceans).
Right, "I think" is an important part here. This is personal opinion, but what does back it?

Micah Zoltu [9:51 PM]
OK, so you are asserting that Iota depends on a global LPAN network to function?

Come-from-Beyond [9:52 PM]
No

[9:52]
My words can be narrowed down to this phrase:
Omnipresence can't be achieved easily

Micah Zoltu [9:53 PM]
I don't believe omnipresence is necessary for what I described above?

Come-from-Beyond [9:53 PM]
A lot of meshnets will go via classical internet, we probably even be unable to distinguish where IoT ends and classical Internet starts

[9:54]
I believe it's necessary because of mesh-like nature of the IOTA network

[9:55]
How would the network react to your attack in slow-motion?

Micah Zoltu [9:55 PM]
Lets imagine the Iota network is made-up up a bunch of isolated mesh networks that are all interconnected via the internet. Lets also imagine that an attacker cannot penetrate (become part of) any one of the individual mesh networks, but they can easily become part of the larger Iota network.

Come-from-Beyond [9:55 PM]
ok

Micah Zoltu [9:56 PM]
Such an attacker can simulate as many mesh network clusters as they want. They can make it look like there are millions of little mesh clusters out there when in reality there are only 1000 + a couple AWS nodes.

Sunny Aggarwal [9:56 PM]
They can just simulate a mesh network

Micah Zoltu [9:57 PM]
So those 1000 legitimate mesh networks connect up to the Iota network and find that they are one of millions of similar little clusters. They don't realize that they are really communicating mostly with a couple AWS nodes.

Come-from-Beyond [9:57 PM]
Why does he need to simulate it? (edited)

[9:58]
I see no reason for him to hide the fact that it's just one supercomputer

Micah Zoltu [9:58 PM]
I'm giving you the benefit of the doubt. All that matters is that you can't measure network size by number of nodes. ¯_(□)_/¯

Ned Kt [9:58 PM]
joined #tanglemath

Micah Zoltu [9:59 PM]
The point of this argument is just to show that node-count is meaningless, only computing resources (CPU/RAM/network) is meaningful. (edited)

Come-from-Beyond [9:59 PM]
Is he connected to most of the nodes of the attacked cluster? (edited)

[9:59]
or only to edge nodes?

Micah Zoltu [10:00 PM]
He connects to any node he can peer with, which means any node that is connected to the network at large and not isolated in a mesh somewhere. (edited)

[10:01]
He does whatever is necessary to increase his connectivity, and the only nodes he cannot connect to are private nodes (nodes that don't connect to any untrusted party).

Come-from-Beyond [10:01 PM]
this connection part is unclear, it sounds like you are talking about IP

[10:02]
does IoT use IP in this scenario?

Micah Zoltu [10:02 PM]
¯_(□)_/¯

[10:02]
Presumably there is _some_ connection to the larger network via IP.

Sunny Aggarwal [10:02 PM]
It doesn’t matter what individual meshes use. As long as they’re still using the internet to connect meshes to each other. (edited)

Micah Zoltu [10:02 PM]
Individual mesh networks can communicate however they want.

Come-from-Beyond [10:02 PM]

Let's put on hold the attack and make sure we are on the same page regarding the connectivity

Micah Zoltu [10:02 PM]
https://iotatangle.slack.com/archives/C3V610ULS/p1497470132025734
Micah Zoltu
Lets imagine the Iota network is made-up up a bunch of isolated mesh networks that are all interconnected via the internet. Lets also imagine that an attacker cannot penetrate (become part of) any one of the individual mesh networks, but they can easily become part of the larger Iota network.
Posted in #tanglemathYesterday at 9:55 PM

[10:03]
Each mesh network is connected _internally_ however they want. Maybe via sonar.
:slightly_smiling_face:

Come-from-Beyond [10:03 PM]
How do you envision communication between nodes of an IoT network?

Sunny Aggarwal [10:03 PM]
It doesn't matter. We're saying how will IoT mesh networks communicate with each other? (edited)

Micah Zoltu [10:04 PM]
Individual nodes can communicate with each other however they want. But in order to connect with the larger IoT network they presumably would go over IP _unless_ there is some other global network available (like a global mesh) which is unrealistic.

[10:04]
And even if there were a global mesh, presumably one
could buy computing power on _that_ network.

cyclux [10:04 PM]
joined #tanglemath

Come-from-Beyond [10:05 PM]
> He connects to any node he can peer with, which means any node that is connected to the network at large and not isolated in a mesh somewhere.
This part is unclear. Look at wiki page with the list of meshnet protocols.

[10:05]
There are a lot of them and none is the silver bullet

Micah Zoltu [10:05 PM]
Doesn't matter.

Come-from-Beyond [10:05 PM]
Actually it does, because you imagine it as IP connection

Mat Tam [10:05 PM]
joined #tanglemath

Micah Zoltu [10:06 PM]
There could be a billion different mechanisms for connecting nodes together. Unless you can _prevent_ me from putting my supercomputer on the network, you can't prevent me from spoofing

nodes.

Come-from-Beyond [10:06 PM]
At this point bandwidth starts playing role

[10:06]
> you can't prevent me from spoofing nodes.
I don't even need to, you can't connect to most of nodes

Micah Zoltu [10:06 PM]
Any individual node can't know what "most of the nodes" is.

Come-from-Beyond [10:07 PM]
This is the problem 5G is trying to solve

[10:07]
How to let all nodes to be connected

[10:07]
unfortunately they can provide connectivity only for 1 device per 1 square meter

[10:07]
which is very low for urban areas

Micah Zoltu [10:08 PM]
And I can put my supercomputer on a 5G network and tell everyone I'm connected to, "I'm connected to a billion nodes!" ¯_(□)_/¯

Come-from-Beyond [10:08 PM]
> you can't prevent me from spoofing nodes.
I disagree with this

Micah Zoltu [10:08 PM]
What prevents me from spoofing nodes?

Come-from-Beyond [10:08 PM]
what _allows_ it?

Sunny Aggarwal [10:09 PM]
That's the whole point of an open and public distributed ledger… That anyone can join. You can't stop someone from creating many Sybil identities. (edited)

Micah Zoltu [10:09 PM]
I tell anyone I'm connected to that I'm _also_ connected to a whole separate mesh behind me that is massive.

Jonathan Allen [10:09 PM]
joined #tanglemath

Come-from-Beyond [10:09 PM]
Look at the problem from the perspective of common sense: A lot of money is spent to allow all devices to be interconnected and you claim it's easy.

Micah Zoltu [10:10 PM]
Perhaps one of us is misunderstanding what a mesh network is.

Come-from-Beyond [10:10 PM]
@sunnya97
> You can’t stop someone from creating many Sybil identities.
In IoT I can. It's standard resource-testing countermeasure which works automatically in IoT.

[10:10]
> Perhaps one of us is misunderstanding what a mesh network is.
Definitely

Micah Zoltu [10:10 PM]
A mesh network, as I understand it, is a network where each node is connected to its neighbors, and nodes in the network can forward information from any of their neighbors to any other of their neighbors.

[10:11]
No node in a mesh network knows about anything _other_ than its neighbors. It must trust (usually via signatures) that anything coming from a neighbor is sourced from some distant node in the network. (edited)

Come-from-Beyond [10:11 PM]
how can you *spoof* some node? (edited)

[10:11]
you need to go to some spot on the earth and place your radiotransmitter

[10:11]
there are no wires going to some superhub

Sunny Aggarwal [10:12 PM]
@come-from-beyond Are you suggesting that there will only be a *single* global mesh network for all IoT devices in the work? (edited)

Micah Zoltu [10:12 PM]
Sure, I go to some spot on earth drop down a radio transmitter and a supercomputer. I tell all my neighbors, "I'm connected to a billion neighbors behind me."

[10:12]
No node can disprove that I am not actually connected to a billion neighbors.

Come-from-Beyond [10:12 PM]
> Are you suggesting that there will only be a *single* global mesh network for all IoT devices in the work?
It depends on level of detalization

[10:13]
> Sure, I go to some spot on earth drop down a radio transmitter and a supercomputer. I tell all my neighbors, "I'm connected to a billion neighbors behind me."
You cannot do it physically.

[10:13]
Because of bandwidth restrictions

Micah Zoltu [10:13 PM]
Why not?

Sunny Aggarwal [10:13 PM]
> It depends on level of detalization
What does this mean? (edited)

Come-from-Beyond [10:13 PM]
I'll draw a pic to show

Micah Zoltu [10:13 PM]
So that means the network doesn't have enough bandwidth to actually support the network.

[10:13]
A mesh network needs enough bandwidth to route everything.

Come-from-Beyond [10:14 PM]
mesh network as a whole

[10:14]
but we are talking about several edge nodes

Micah Zoltu [10:14 PM]
Now if you truly have a global mesh network, you can argue that any single route has very limited bandwidth but you can take multiple routes to achieve higher bandwidth.

[10:15]
But that _requires_ a single global mesh network that doesn't have any other backbone (e.g., internet).

[10:15]
As soon as you have a backbone, a supercomputer can sit on that backbone and simulate whatever he wants. (edited)

Come-from-Beyond [10:16 PM]
It can't because bandwidth is limited

Micah Zoltu [10:16 PM]
So _either_ you are asserting that Iota depends on a global backbone-free mesh network _or_ you have to accept that one can run a supercomputer on that backbone.

Come-from-Beyond [10:16 PM]
you need 1 million connections

[10:16]
you can't push whole ocean via small river

[10:16]
you need 1000 rivers for that

Micah Zoltu [10:17 PM]
Sure, _if_ you have a single global mesh network that has no backbone.

[10:17]
Such a thing does not exist today.

Come-from-Beyond [10:17 PM]
already exist in different hypostases

[10:17]
let me google it for you

Micah Zoltu [10:18 PM]
The _no backbone_ bit is critically important.

[10:18]
A bunch of isolated mesh networks that connect to each other over the internet doesn't count as a global mesh network for the sake of your argument of "not enough bandwidth".

Come-from-Beyond [10:19 PM]
https://www.geckoandfly.com/22562/chat-without-internet-connection-mesh-network/ (edited)

Micah Zoltu [10:19 PM]
Those can't hop the Pacific ocean without a single backbone.

Come-from-Beyond [10:20 PM]
Isolated meshnets are isolated, not much can be done before they converge

Micah Zoltu [10:20 PM]
You can create an isolated mesh network with tech like that, but not a global backbone free network.

Come-from-Beyond [10:21 PM]
It's not obvious so some extra arguments should be provided

Micah Zoltu [10:21 PM]
Which part isn't obvious?

Come-from-Beyond [10:21 PM]
> but not a global backbone free network.
(edited)

xula [10:22 PM]
joined #tanglemath

Micah Zoltu [10:22 PM]
(will be slow to respond, have a meeting)

[10:22]
So lets say I have a mesh network that spans all of North America. I want to connect that mesh network to a similar continent-wide mesh network in Europe. I need some kind of backbone to connect NA to EU.

Sunny Aggarwal [10:22 PM]
> Isolated meshnets are isolated, not much can be done before they converge
How do they plan on converging?

Come-from-Beyond [10:23 PM]
they don't plan, it just happens eventually

[10:23]
or doesn't happen

Michael M [10:24 PM]
joined #tanglemath

Micah Zoltu [10:24 PM]
The technology doesn't exist that allows a node in NA to connect to a node in EU without going over something like a Satellite or underwater cables or microwave. These things are all necessarily high-bandwidth solutions because they are incredibly expensive pieces of infrastructure that are _huge_ economies of scale.

Come-from-Beyond [10:25 PM]
they will likely go via classical internet routes

Micah Zoltu [10:25 PM]
:point_up: Right. This is the backbone I talk about.

Sunny Aggarwal [10:27 PM]
Exactly! This is what we've been trying to say. You need to use the internet to connect multiple mesh networks together.

Come-from-Beyond [10:27 PM]
and?

rta [10:28 PM]
joined #tanglemath

Come-from-Beyond [10:28 PM]
Let's use concrete numbers

Sunny Aggarwal [10:28 PM]
The protections that the network topography of the mesh network offer don't apply anymore when dealing with an inter-mesh Tangle

Come-from-Beyond [10:28 PM]
We have 1000 nodes in our cluster

[10:28]
10 of the nodes are connected to Internet

[10:28]
So txs from other clusters leak via them

[10:29]
Your turn

projectShift (Ricardo)
[10:30 PM]
:partyparrot:

Sunny Aggarwal [10:33 PM]
Sure so any transactions that happen within that 1000-node cluster are “safe”. But anything coming in from outside that cluster (through the 10 gateway nodes) are susceptible to the supercomputer

Come-from-Beyond [10:34 PM]
alright, now we need @micah.zoltu to agree with you and we will move to another attack scenario where supercomputer attacks _other_ clusters

Micah Zoltu [10:34 PM]
(on a call, but agree with that statement) (edited)

Come-from-Beyond [10:35 PM]
great, I was thinking you were going to attack transactions inside the cluster, this is what caused the misunderstanding, it seems

[10:36]
so, 1000 nodes, 10 nodes on the edge, how would you attack transactions generated by _other_ clusters?

Micah Zoltu [10:36 PM]
You don't attack _transactions_, you just run a supercomputer that is generating 10x as much as the rest of the network.

David Castella [10:36 PM]
joined #tanglemath

Micah Zoltu [10:37 PM]
Or more specifically, 34% (more than the threshold you indicated was required to attack the network). (edited)

Karsten Wahn [10:37 PM]
joined #tanglemath. Also, @panzki joined.

Micah Zoltu [10:39 PM]
Those 1000 IoT devices are no match for my one supercomputer. I can easily take-over 34% of the network power by any metric (CPU, RAM, bandwidth, etc.).

[10:39]
And if necessary, I can _pretend_ my supercomputer is really a 3000-node mesh net with 30 edge points. (3x as big as the 1000 node mesh with 10 edges) (edited)

Come-from-Beyond [10:39 PM]
which 1000 devices? of
our cluster or some other cluster?

Micah Zoltu [10:40 PM]
https://iotatangle.slack.com/archives/C3V610ULS/p1497472569862049
Come-from-Beyond
so, 1000 nodes, 10 nodes on the edge, how would you attack transactions generated by _other_ clusters?
Posted in #tanglemathYesterday at 10:36 PM

Come-from-Beyond [10:40 PM]
you connected to 10 edge nodes and push a lot of txs?

Micah Zoltu [10:40 PM]
Yeah.

Come-from-Beyond [10:41 PM]
but these 10 nodes can't push your txs with the same rate

[10:41]
only 10% of your txs will be pushed thru

Micah Zoltu [10:41 PM]
That means that those 10 nodes _can't_ support connecting to the network unless their sub-mesh makes up the _majority_ of the network.

[10:42]
That 1000-node mesh network with 10 edges _must_ be able to handle traffic from the rest of the network, which is _very likely_ bigger than them.

[10:42]
Ignoring attackers entirely. They need to be able to connect to the larger network as a whole. They can't assume that their mesh is the largest part of the network. (edited)

Come-from-Beyond [10:43 PM]
when we said "cluster" it already assumed that we have some parts of the global network isolated

[10:43]
have you just claimed that snow is white when we already agreed on that?

Micah Zoltu [10:43 PM]
Not sure what you are referring to?

Come-from-Beyond [10:44 PM]
well, probably bad analogue

Micah Zoltu [10:44 PM]
I'm discussing a 1000-node cluster with 10 edges. This cluster wants to talk to the _rest_ of the world-wide network. It does this via those 10 edge nodes.

Come-from-Beyond [10:44 PM]

cluster is separated from another part of the global network

Micah Zoltu [10:45 PM]
That means those 10 edge-nodes need to be able to handle the traffic of the rest of the global network, or else the cluster will not be able to stay in-sync with the rest of the network.

Come-from-Beyond [10:45 PM]
if the bandwidth between clusters is too "narrow" then they will never converge

Nate Rush [10:45 PM]
joined #tanglemath

Micah Zoltu [10:45 PM]
Which means we _must_ accept that those 10 edge nodes _can_ handle the bandwidth required for the rest of the global network.

[10:46]
If not, then they will not be able to be part of the global network, they will always be isolated and behind (never converge).

Sunny Aggarwal [10:46 PM]
So then _either_ they will never converge or they're susceptible to the supercomputer.

Come-from-Beyond [10:46 PM]
if traffic is too large then we'll have isolated parts, it's applicable to every single cryptocurrency

Micah Zoltu [10:46 PM]
You are the one that argued they don't have enough bandwidth. :slightly_smiling_face:

[10:47]
So, if those 10 edge nodes _can_ handle the bandwidth required to participate in the global network then a supercomputer can _simulate_ the global network (or a significant portion of it) and that cluster will be none the wiser.

Come-from-Beyond [10:48 PM]
I still not sure I get the attack vector. Spam attack? There is no prevention, just read articles like https://en.wikipedia.org/wiki/2016_Dyn_cyberattack (edited)

Sunny Aggarwal [10:48 PM]
> if traffic is too large then we'll have isolated parts, it's applicable to every single cryptocurrency
But other cryptocurrencies aren't depending on large traffic, network inefficiencies, and isolated subnetworks for security. You're suggesting that Iota is. (edited)

Micah Zoltu [10:49 PM]
The last hour of debate was just arguing against your claim that one can't simulate nodes.

Come-from-Beyond [10:49 PM]
Yes, because you can't connect to most of the nodes

Micah Zoltu [10:49 PM]
The above argument _just_ asserts that node simulation is possible and node-count is a meaningless

number since anyone can simulate nodes on the _global_ network trivially.

Come-from-Beyond [10:49 PM]
you can connect to some part of it

[10:50]
start spamming

Micah Zoltu [10:50 PM]
Sure, but the parts we connect to will propagate our simulated nodes.

Come-from-Beyond [10:50 PM]
and bringing _several_ nodes down

Micah Zoltu [10:50 PM]
If they can't handle traffic from the global network, they aren't actually part of the network.

[10:50]
https://iotatangle.slack.com/archives/C3V610ULS/p1497473147054289
Micah Zoltu
Which means we _must_ accept that those 10 edge nodes _can_ handle the bandwidth required for the rest of the global network.
Posted in #tanglemathYesterday at 10:45 PM

[10:51]
Either your cluster can handle the traffic of the global network via its 10 edges or it can't. If it can't, then it isn't part of the global Iota tangle and doesn't matter. Its effectively running a fork of the network and we don't care about it.

[10:51]
If it _can_ keep up via those 10 edges then it is susceptible to supercomputer node simulation _via_ those edges.

Come-from-Beyond [10:52 PM]
agree, looks like you are telling me what I already know

[10:52]
let's sync before continuing

Micah Zoltu [10:52 PM]
* Isolated cluster of 1000 nodes, 10 of which are edge nodes.
* Edge nodes connect to global Iota network over something like IP (or similar high bandwidth centralized route that anyone can get on).
* Cluster _can_ handle bandwidth requirements of the global network via those edge nodes. (edited)

Sunny Aggarwal [10:53 PM]
And the thing is, this itself in a way *is* the exact attack we were suggesting. If the supercomputer can force a mesh into being isolated from the tangle, it can then start charging fees in order to allow it to communicate with the rest of the larger network

Come-from-Beyond [10:53 PM]
https://iotatangle.slack.com/archives/C3V610ULS/p1497472386799832

https://iotatangle.slack.com/archives/C3V610ULS/p1497472447820424
https://iotatangle.slack.com/archives/C3V610ULS/p1497472460824929
Sunny Aggarwal
Sure so any transactions that happen within that 1000-node cluster are “safe”. But anything coming in from outside that cluster (through the 10 gateway nodes) are susceptible to the supercomputer
Posted in #tanglemathYesterday at 10:33 PM
Come-from-Beyond
alright, now we need @micah.zoltu to agree with you and we will move to another attack scenario where supercomputer attacks _other_ clusters
Posted in #tanglemathYesterday at 10:34 PM
Micah Zoltu
(on a call, but agree with that statement)
Posted in #tanglemathYesterday at 10:34 PM

[10:53]
Is the above correct?

Micah Zoltu [10:54 PM]
Yes.

Come-from-Beyond [10:54 PM]
@sunnya97 ?

Sunny Aggarwal [10:54 PM]
Yes.

Micah Zoltu [10:54 PM]
With the caveat on what "safe" means?

[10:54]
If by safe you just mean that they can send transactions amongst each other, sure.

Come-from-Beyond [10:54 PM]
Now tell me how can you attack when our cluster covers 90% of the earth.

Micah Zoltu [10:54 PM]
How did you jump to that?

Come-from-Beyond [10:54 PM]
it's just an assumption (edited)

Swifty Pancake [10:54 PM]
joined #tanglemath

Micah Zoltu [10:55 PM]
The technology doesn't exist to have a mesh network cross oceans without a backbone.

Sunny Aggarwal [10:55 PM]
Well for one I promise you your cluster won’t cover 90% of the earth because 70% of it is water. (edited)

uvas [10:55 PM]

90% of the land I imagine he meant

Micah Zoltu [10:55 PM]
At best you could have 4 major mesh networks (NA, SA, EU/Asia, Africa) with a collection of minor mesh networks in various island clusters.

Come-from-Beyond [10:56 PM]
So, to make it clear:
Your attack works if our cluster can't cover 90% of the earth.
Your attack does NOT work if our cluster can cover 90% of the reath.
Agree?

Micah Zoltu [10:56 PM]
I am not currently _thinking_ about an attack against a _global_ and backbone free mesh network. For the sake of this discussion, I propose we ignore it.

[10:57]
If you believe a 90% backbone free mesh network is a realistic dependency of Iota, then we should discuss _that_ instead.

Come-from-Beyond [10:57 PM]
Guys, I need your both to say only AGREE or DISAGREE to
https://iotatangle.slack.com/archives/C3V610ULS/p1497473775265357
Come-from-Beyond
So, to make it clear:
Your attack works if our cluster can't cover 90% of the earth.
Your attack does NOT work if our cluster can cover 90% of the reath.
Agree?
Posted in #tanglemathYesterday at 10:56 PM

Micah Zoltu [10:57 PM]
If you don't believe that is a realistic dependency, we can ignore it for this discussion.

Come-from-Beyond [10:57 PM]
Let's do it in few smaller steps

[10:58]
@sunnya97 ?

Micah Zoltu [10:58 PM]
I cannot assert whether the attack works against a 90% global backbone free mesh network because I haven't thought about it. I don't intend to think about it because I think that is an unrealistic requirement.

Sunny Aggarwal [10:58 PM]
I don’t think its worth spending time to think about whether attacks in that system are possible, because such a network is absurd and infeasible.

Come-from-Beyond [10:59 PM]
@micah.zoltu Now it looks to me that you are trying to evade giving a direct answer to a direct question.

Micah Zoltu [10:59 PM]
I gave you a direct answer.

[10:59]
If you do think that 90% global coverage backbone free global mesh network is possible then we should discuss that.

Come-from-Beyond [10:59 PM]
@sunnya97 this is applied to you too

Sunny Aggarwal [10:59 PM]
Our answer to that is “We don’t know”

Come-from-Beyond [10:59 PM]
@here, I need someone as a referee

[11:00]
I asked a direct question and the both counterparties refuse to give a direct answer

[11:00]
to me it doesn't look very good

[11:00]
c'mon guys, either you argue in a civilized manner or we stop this

Micah Zoltu [11:00 PM]
Not sure what you want from us. "I don't know" is a reasonable answer to a question.

Tristan [11:00 PM]
:popcorn:

[11:00]
:dark_sunglasses:

Come-from-Beyond [11:00 PM]
Let me repeat all again

[11:01]
https://iotatangle.slack.com/archives/C3V610ULS/p1497472386799832
https://iotatangle.slack.com/archives/C3V610ULS/p1497472447820424
https://iotatangle.slack.com/archives/C3V610ULS/p1497472460824929

Paul
H [11:01 PM]
@winston be ref

Sunny Aggarwal [11:01 PM]
Hold on. There’s a debate fallacy for this. Give me a sec.

Come-from-Beyond [11:01 PM]

uh, Slack refused to unfold the links...

[11:01]
ok, I give you 1 hour

Micah Zoltu [11:01 PM]
I think it won't unfold them multiple times in a short period.

cyclux [11:02 PM]
slack has issues I think right now. Images are also not loading well

Micah Zoltu [11:02 PM]
Perhaps it will help if I modify my original argument:
1. Given that a global mesh network is not possible with today's technology.
2. A motivated actor in the Iota system can simulate as many nodes as it wants.

[11:02]
If you disagree with (1) then we should discuss that.

Come-from-Beyond [11:02 PM]
@micah.zoltu revise our convo too, you can take back some words if you wish

[11:02]
I'll come here again in ~1 hour

Micah Zoltu [11:02 PM]
I'm not taking back anything, just adding an assertion that I thought was implicit but sounds like it isn't.

Come-from-Beyond [11:02 PM]
some other stuff requires my attention

[11:03]
let's continue in 1 hour

Sunny Aggarwal [11:05 PM]
Ahh found it. It’s called the existential fallacy.

[11:05]
Here’s a screenshot from the description of a podcast I listen to

Sunny Aggarwal [11:06 PM]
uploaded this image: 19212720_10207222792088509_328176056_o.png
Add Comment

Micah Zoltu [11:06 PM]
https://en.wikipedia.org/wiki/Existential_fallacy (edited)

uvas [11:11 PM]
this is an interesting conversation, but can i squeeze a quick question in? I was sent here form iota-learn

Micah Zoltu [11:12 PM]
I believe we are on a 1-hour break anyway. :smile:

uvas [11:12 PM]
oh great. I was wondering about wallet security. Is there anything to prevent someone from plinking away on the wallet with random seeds hoping to hit a jackpot?

Micah Zoltu [11:13 PM]
No, but it would take them a billion years or something to find _one_ account. (edited)

Hoediur [11:13 PM]
joined #tanglemath

uvas [11:13 PM]
yea, ridiculously large numbers involved

Micah Zoltu [11:13 PM]
Same as things for Bitcoin/Ethereum accounts.

Paul H [11:13 PM]
or you would have to use a seed like "PASSWORD"

uvas [11:13 PM]
lolz

Paul H [11:14 PM]
or something else incredibly stupid

Micah Zoltu [11:14 PM]
Your seed should _always_ be generated by a computer. :slightly_smiling_face:

uvas [11:14 PM]
Yea, i tried a shorter seed but wallet wouldnt accept it

[11:14]
do they all have to be 81 long?

cyclux [11:15 PM]
I also have a question about the lightwallet: How is the seed sent to the server? Plain text (I hope not :wink:) ?

Tristan [11:15 PM]
So, this is all over my head. But are you guys basically describing a spam/51% attack?

Alon Elmaliah [11:15 PM]
the seed never leaves your machine ^

uvas [11:15 PM]
i was told seeds never leave your wallet

cyclux [11:17 PM]
@alon.elmaliah ok, makes sense , because the calc is done locally I guess

Winston [11:18 PM]
CfB's assumption is that at time t+1 most of the landmass on planet Earth will be covered in mesh nets (I'm still unclear on how this averts the inter-continental IP access points, according to Micah and Sunny's proposed supercomputer mesh simulation attack vector). However at time t, in an environment with no existing mesh nets (now), it seems as though this assumption would not apply.

Unless CfB is trying to prove a point by establishing t+1, in which case he's just taking his sweet time. Ha. Looking forward to the continuation of this discussion. (edited)

dgsus [11:20 PM]
joined #tanglemath

Micah Zoltu [11:20 PM]
> most of the landmass on planet Earth will be covered in mesh nets (I'm still unclear on how this averts the inter-continental IP access points, according to Micah and Sunny's proposed supercomputer mesh simulation).
I _believe_ he is arguing that most of the landmass of earth is covered in a _single_ meshnet. Not multiple meshnets.

[11:20]
If you have multiple meshnets connected via a backbone then our attack works.

[11:21]
(e.g., EU meshnet connected to NA meshnet via trans-pacific internet backbone cables) (edited)

Winston [11:21 PM]
The attack works from between time t until just before achieving t+1. Even given a single meshnet at t+1 (edited)

[11:22]
Hardware implementation & adoption doesn't happen overnight

Micah Zoltu [11:23 PM]
Yeah.

[11:23]
And science doesn't happen overnight. :smile:

[11:24]
I don't believe there exists technology to allow for crossing oceans with a low-bandwidth and low-infrastructure cost mesh type network connection.

[11:24]
Satellite, fiber, microwave are all I know of, all of which are _massively_ expensive pieces of infrastructure for cross-ocean connections.

Winston [11:24 PM]
That doesn't matter. This discussion needs to be happening in the context of 't' (edited)

Micah Zoltu [11:25 PM]
Agreed.

Jonathan Allen [11:26 PM]
I think that this would apply: https://arstechnica.com/information-technology/2016/11/spacex-plans-worldwide-satellite-internet-with-low-latency-gigabit-speed/ but I totally agree that the conversation should focus on 't' as that is what most individuals are concerned with, not what could possibly happen in 5-10 years. (edited)

Friedrich E. [11:26 PM]
joined #tanglemath

Fahad Sheikh [11:27 PM]
Someone take this whole discussion and post it in the forum plz. I'm at work. Wouldn't want to lose this. Most people don't understand the Tangle and its security, this could be sufficient discussion for that.

Fahad Sheikh [11:27 PM]
Call it "IOTA Consensus and Security" perhaps.
2 replies Last reply about 11 hours ago View thread

Micah Zoltu [11:28 PM]
@jon.allen I believe that such a network wouldn't qualify as `t+1` for the sake of the argument that CfB is making.

[11:29]
Such a network would have enough between-node bandwidth to handle all of Iota, plus individual clusters wouldn't be private networks.

[11:30]
I actually hope I fail too. I _want_ to be convinced that I'm wrong. :smile: I _want_ a tangle to work. (edited)

Sunny Aggarwal [11:31 PM]
Yeah, it also just doesn't make any sense that we will build a brand new *global* communications infrastructure that is *purposefully* worse and less efficient than our current one because a Tangle depends on this inefficiency for security (edited)

Jonathan Allen [11:33 PM]
I feel like all of that is off topic. For the sake of argument I would love to see how CFB qualifies his 90% statement and where he goes with it but the focus of this conversation should be on how the network could be attacked in the next 6-12 months.

Sunny Aggarwal [11:34 PM]
Short aside: @winston or whomever does the archiving for this channel, take a look at http://slackarchive.io/. We use it for our Blockchain at Berkeley slack and it works quite well.

2 replies Last reply about 11 hours ago View thread

Andreas Osowski [11:37 PM]
How would you define the simulation by a supercomputer?

Come-from-Beyond [11:39 PM]
@micah.zoltu @sunnya97 I'm back to our unicorn. Before we continue I'd like to remind about https://iotatangle.slack.com/archives/C3V610ULS/p1497469446793309
Fahad Sheikh
just a suggestion. The discussion in Tanglemath should somehow be saved and posted in the forum. Because this is the very discussion that people want to read to see how technically sound the Tangle is. Or you should only do it in the forum :slightly_smiling_face:
Posted in #tanglemathYesterday at 9:44 PM

[11:39]
Can we continue now?

Sunny Aggarwal [11:40 PM]
@micah.zoltu ready for round 2 haha?
Or actually more like round 3 for me. Round 4 for you? (edited)

dylan [11:41 PM]
I'm probably not in the best place to comment, but oh well. Even if we assume that at some point t+1 we'll have the technology able to create a single backbone-free global mesh network, we would have to go from t to t+1. If at any point during that time the network is found to be susceptible to an attack, the security of the proposed t+1 system wouldn't matter. It most likely wouldn't be adopted unless at the point in which this global mesh network is possible, everyone implements simultaneously. So, unless the system at t can be defended, future predictions wouldn't matter

Come-from-Beyond [11:43 PM]
So... To make sure: If I pull out of my sleeve such network you both lose the dispute, right?

Micah Zoltu [11:43 PM]
I would have to think more on the topic if you managed to do that.

[11:43]
I haven't spent any time considering how Iota would behave in the face of a global backbone-free mesh network.

[11:44]
It is possible that the problems I have been discussing would no longer work, but it is also possible they would.

Come-from-Beyond [11:45 PM]
Can I have your answers on the question in the very end?

``` Sunny Aggarwal
Sure so any transactions that happen within that 1000-node cluster are "safe".  But anything coming in from outside that cluster (through the 10 gateway nodes) are susceptible to the supercomputer
```

Come-from-Beyond
alright, now we need @micah.zoltu to agree with you and we will move to another attack scenario where supercomputer attacks _other_ clusters

Micah Zoltu
(on a call, but agree with that statement)

...

Come-from-Beyond [11:56 PM]
So, to make it clear:
Your attack works if our cluster can't cover 90% of the earth.
Your attack does NOT work if our cluster can cover 90% of the reath.
Agree?```

Micah Zoltu [11:46 PM]
sigh we have answered you several times.

Come-from-Beyond [11:46 PM]
Just Agree or Disagree

Micah Zoltu [11:46 PM]
I'm not sure what you want from us. I'm not going to blindly agree to something I have spent _zero_ time considering.

Come-from-Beyond [11:46 PM]
I can give you more time

[11:46]
but this will be continued tomorrow only

lazarus blackwater [11:46 PM]
joined #tanglemath

Micah Zoltu [11:46 PM]
I have no intention of spending my time thinking about
how Iota will function in the face of Unicorns.

[11:47]
Either you can argue that Unicorns are real and if successful I will consider it, or we can just end the conversation, or we can discuss Iota in a world without unicorns.

Jonathan Allen [11:47 PM]
Why not just agree and see if evidence can be provided for this assertion? All this posturing and qualifying is such a waste of time. Your answer isn't legally binding, you can change your answer if your opinion changes.

Come-from-Beyond [11:47 PM]
@micah.zoltu I really starting thinking that we'll never be able to argue ever again. It's because you evade direct questions that may lead to your loss in a dispute (edited)

Hazelnuts [11:48 PM]
Side question, does iota not utilise an incremental nonce when signing transactions?

Fahad Sheikh [11:48 PM]
CFB, why is it a precondition to get an answer of a network that doesn't exist? Why can't the argument be from the perspective of an existing reality? Lets say the answer is agree to that question. Lets move on :slightly_smiling_face:

Micah Zoltu [11:48 PM]
@jon.allen Because I have a sneaking suspicion that he is going to use my agreement against me in another argument, or that he _will_ be able to convince me of a global backbone-free network and then throw my agreement in my face (despite me never having actually given it thought).

Come-from-Beyond [11:49 PM]
> Why can't the argument be from the perspective of an existing reality?
I'll pull this network right after the both opponents give me direct answers

Andreas Osowski [11:50 PM]
Wouldn't the supercomputer be susceptible to the same network congestion though given that he's only able to interface with the backbone via a limited set of nodes and probably not connected to most of the nodes out there? Or was that the 33% assumption?

Fahad Sheikh [11:50 PM]
Micah why don't you just agree for now, and then you can disagree later after you put some thought to it, if required. Lets continue.

Micah Zoltu [11:51 PM]
@come-from-beyond You are making the following logical fallacy:
https://en.wikipedia.org/wiki/Existential_fallacy (edited)

Come-from-Beyond [11:51 PM]
@micah.zoltu I don't want to put too much pressure on you but you should decide...

Sunny Aggarwal [11:51 PM]
We're not here as opponents. We're here to figure out the best path forward for Iota and the Blockchain ecosystem :)

Micah Zoltu [11:51 PM]
@hellsingfan I'm not particularly interested in continuing a discussion with someone who is going to force me into a corner via logical fallacies.

Jae Kim [11:52 PM]
joined #tanglemath

Come-from-Beyond [11:52 PM]
@sunnya97 you are smart guy too, I'll be doubleupset if I lose opportunity to argue with you again in the future...

Fahad Sheikh [11:52 PM]
Then it shouldn't matter. Lets explore both agree and disagree as valid choices. Assume its agree for

now?

Sunny Aggarwal [11:52 PM]
But okay @jon.allen and @hellsingfan are right

Micah Zoltu [11:52 PM]
If continuing this discussion requires me to _lie_ to have it continue, then I'm not interested in continuing.

Sunny Aggarwal [11:52 PM]
I agree.

Come-from-Beyond [11:52 PM]
@micah.zoltu pity, but nothing can be done then

Andreas Osowski [11:52 PM]
If CFB uses logical fallacies, then this is a public conversation and everybody will _know_ that he can only win the argument using such fallacies. So both of you have something to lose. Why not just continue ....

Come-from-Beyond [11:52 PM]
@sunnya97 Do you remember I mentioned that we use manual tethering?

Stas [11:52 PM]
joined #tanglemath

Micah Zoltu [11:53 PM]
@th0br0 I'm willing to continue, but I'm not going to agree to a statement I don't agree with. :slightly_smiling_face:

Come-from-Beyond [11:53 PM]
It happened shortly before you went to sleep

Sunny Aggarwal [11:53 PM]
Yeah

Fahad Sheikh [11:53 PM]
You're not 'agreeing'. You're 'agreeing for the sake of argument'. There is a distinction. You've made your hesitation clear, no one will hold it against you.

Johnny Bender
[11:53 PM]
joined #tanglemath

Come-from-Beyond [11:54 PM]
The purpose of that tethering (instead of peer autodiscovery) was to get the same properties as IoT meshnets get

Dhruv Kumar [11:54 PM]
joined #tanglemath. Also, @albert joined, @moke joined.

Come-from-Beyond [11:54 PM]
Right now we have global meshnet mimicked by our nodes

imi
[11:54 PM]
joined #tanglemath

Micah Zoltu [11:54 PM]
What you are proposing is a global web of trust.

[11:55]
"I will only peer with people I trust."

Bern [11:55 PM]
joined #tanglemath

Micah Zoltu [11:55 PM]
The problem is, it only takes _one_ break in the entire global web of trust chain to undermine the trust network.

Come-from-Beyond [11:55 PM]
@sunnya97 apply the supercomputer attack on it, please. In mind of coz, not in reality.

[11:55]
Will your attack be successful?

Sunny Aggarwal [11:56 PM]
Essentially this is close to a permissioned system then.

Micah Zoltu [11:56 PM]
All I need to do is get one other "edge" node to trust me and I can now simulate an entire network.

David Sønstebø [11:56 PM]
Can either of you just prove your attacks and collect major bug bounties? alternatively shut the fuck up? It's pretty simple; if you think you got an attack vector, then prove it

Come-from-Beyond [11:56 PM]
@sunnya97 we can discuss it later, apply the attack

Micah Zoltu [11:56 PM]
@david We have been trying to for some time.

Come-from-Beyond [11:56 PM]
will it work or NOT?

Micah Zoltu [11:56 PM]
@come-from-beyond Yes, see my above statement.

matthias [11:56 PM]
joined #tanglemath

Come-from-Beyond [11:56 PM]
@micah.zoltu sorry, I'm not going to argue with you anymore

Micah Zoltu [11:57 PM]
¯_(□)_/¯

Fahad Sheikh [11:57 PM]
@david let CFB handle it. Most people are trying to understand Tangle, let this conclude. Its good for IOTA :slightly_smiling_face:

Andreas Osowski [11:57 PM]
@micah.zoltu but the break is susceptible to having limited connectivity to the network, so the preposition is that the wieght of the supercomputer outweighs the rest of the network which would mean that the connection between supercomputer<->rest is higher than the interconnectedness of the network?

Kamal Mokeddem [11:57 PM]
Is there any way to see the current network hashrate?
+1 11 replies Last reply today at 12:01 AM View thread

dylan [11:58 PM]
@david how can you prove an attack vector that requires you to have a super computer? I doubt anyone here has the computational power to do so right now. that does not mean that it is impossible because such computing technology already exists, i.e. quantum

Micah Zoltu [11:58 PM]
@th0br0 Yes. What is being proposed is that there is an off-chain mechanism for building a web of trust such that there is no sufficiently high-bandwidth route into the network from an attacker.

Come-from-Beyond [11:58 PM]
@sunnya97 take as much time as you need, it's not urgent

Micah Zoltu [11:58 PM]
I would be interested in hearing how one builds such a web in the first place.

Come-from-Beyond [11:58 PM]
just ping me so I will get the notification

Andreas Osowski [11:59 PM]
Right. But doesn't this become unfeasible if the network has reached a certain size given the upper limit of the backbone's bandwith?

Micah Zoltu [11:59 PM]
@th0br0 or @come-from-beyond Do you believe that you have a mechanism for building a globally distributed web of trust such that the network as a whole has enough bandwidth but is not susceptible to an untrusted actor gaining a foothold in the network?

----- Today June 15th, 2017 -----
[12:00]
Webs of trust are notoriously hard and unsolved problems. If you believe you have the ability to

build a single _global_ web of trust then _that_ is a major breakthrough. (edited)

[12:01]
I haven't seen any documentation on how you intend to build this web of trust though. At the moment, it isn't a trustful web at all. It is just a slack channel where random people share their IP address with other random people.

Norman Rennhack [12:02 AM]
joined #tanglemath

Andreas Osowski [12:04 AM]
@micah.zoltu Just trying to understand both sides here. Your attack is a much better wording of what I had been thinking about in the past as well. Just to be sure: what's the attacker's goal? Destabilizing the network or injecting false transactions?

Micah Zoltu [12:04 AM]
I actually haven't been proposing a specific attack at all this whole time. I have been merely proposing that the network doesn't achieve the proposed stable equilibrium.

Winston [12:04 AM]
It all stemmed from a selfish tip selection process

[12:05]
I wish CfB could just discuss. It's not an argument

Micah Zoltu [12:05 AM]
The whitepaper describes a particular parent selection strategy and then _defends_ a number of attacks based on that assumption. I started the argument by asserting that the parent selection strategy would not be the dominant one because there are more selfish parent selection strategies available.

Andreas Osowski [12:05 AM]
@winston yeah :confused:

Micah Zoltu [12:06 AM]
This lead down a long winding path that eventually landed us where we are now, which appears to be an assertion that Iota participants will be able to build a decentralized web of trust that is resilient to any non-altruistic actor participating with an arbitrarily large amount of computing power. (edited)

Dhruv Kumar [12:07 AM]
umm why is CfB baring the load of defending this, I am sure the devs on iota could clarify the math?

Kamal Mokeddem [12:07 AM]
I'm looking at how you secure the network against a denial of service attack. What prevents someone from only selecting their own tips and spamming the network with transactions such that the honest tips are orphaned?

David Sønstebø [12:07 AM]
@micah.zoltu I love you input, but why not simply carry out the attack? One demonstration is worth more than 1000 presentations

1 reply Today at 12:09 AM View thread

Micah Zoltu [12:07 AM]
At this point, it is unclear if the web of trust is _actually_ necessary as I have lost track of all of the connections, but it _seems_ to be the linchpin for @come-from-beyond's arguments so I'm trying to validate it.

Winston [12:08 AM]
This slack channel is for discussion. In my estimation, potential attack vectors fit well within the confines of #tanglemath. I guess I could be wrong on my content assumptions though (edited)

Sunny Aggarwal [12:09 AM]
@moke exactly. You can use an ongoing denial of service attack to hold the network hostage as such in order to force people to pay you fees in order to allow their transactions in

Micah Zoltu [12:09 AM]
@david At the moment, the COO (centralized service) defends against all attacks. That being said, I _again_ am not proposing a specific attack (though I have eluded to some such as holding the network hostage as @sunnya97 has described). I'm merely arguing that the whitepaper is flawed.

Fahad Sheikh [12:10 AM]
given that the network barely has any tps, couldn't you try to pull this off even with something less than a supercomputer?

Micah Zoltu [12:10 AM]
Also, I _originally_ felt that it would be more beneficial to discuss the attack with the development team rather than launching a malicious attack against the main network. (edited)

[12:11]
At the moment though, I'm finding some resistance to such discussions, which is eroding at any guilt I may have suffered at executing such an attack. :slightly_smiling_face:

Dhruv Kumar [12:11 AM]
And we are speculating you will follow up with the devs next ^

Micah Zoltu [12:11 AM]
I have been operating under the assumption that some subset of the people involved in this conversation _are_ IOTA devs?

Fahad Sheikh [12:12 AM]
Obviously yo know, and its not even an assumption.

Micah Zoltu [12:12 AM]
Perhaps I just once again find myself arguing against the internet in some obscure corner that no one watches. :smile:

Dhruv Kumar [12:12 AM]
so have we, but that line is not very clear.

Andreas Osowski [12:12 AM]
@micah.zoltu only cfb and david sonstebo.

But if you were to have a SC with a higher hashing rate, as there's nothing to be mined, what would be that SC's goal.

Kamal Mokeddem [12:12 AM]
I'm trying to understand the economic argument for why the network doesn't become more susceptible to denial of service as it grows. It seems that it would have to be centralized forever as network value scales with the square of number of nodes, but proof of work done is only going to rise linearly with number of nodes.

Sunny Aggarwal [12:12 AM]
I thought @come-from-beyond was a dev?

Winston [12:12 AM]
CfB, Paul, and Dr. Popov are in and out of this channel. EDIT: watch @paulh (edited)

Dhruv Kumar [12:13 AM]
and Winston you?

Winston [12:13 AM]
No

Micah Zoltu [12:13 AM]
@th0br0 Off the top of my head, one could hold the network hostage as @sunnya97 suggested. A simpler option would be simply to short IOTA on an exchange and then hold the network hostage for a day or two. (edited)

raganius (Ivan Liborio)
[12:13 AM]
It would be nice to see such attacks on the Tangle. No better way to prove the theory.
You proponents of the attacks could have been doing it since long, if you had honest intentions to help improve the tech. (edited)

Limo Tangleblog.com
[12:14 AM]
as long as the big discussion is on hold, do you mind giving me an elif about the problem?
7 replies Last reply today at 12:17 AM View thread

Andreas Osowski [12:14 AM]
@micah.zoltu hostage because you're saturating the bandwith and hope that the bandwith of the edges you're connected to is higher than that of the remaining network?

Micah Zoltu [12:14 AM]
@raganius As I have told others, I am not actually proposing a particular attack. At the moment I'm only arguing that the whitepaper assumptions are incorrect which invalidate its proofs.

[12:14]
@th0br0 Hostage in the sense of preventing any transactions from "confirming".

raganius (Ivan Liborio)
[12:15 AM]
Too much talk is not the way to go, IMO

Micah Zoltu [12:15 AM]
@limo https://iotatangle.slack.com/archives/C3V610ULS/p1497477929445557
Micah Zoltu
The whitepaper describes a particular parent selection strategy and then _defends_ a number of attacks based on that assumption. I started the argument by asserting that the parent selection strategy would not be the dominant one because there are more selfish parent selection strategies available.
Posted in #tanglemathToday at 12:05 AM

Andreas Osowski [12:15 AM]
@micah.zoltu right. forgot that confirmation != PoW

[12:15]
or is it? too late.

Micah Zoltu [12:16 AM]
Right now confirmation is done by the COO. I believe the whitepaper describes a different confirmation technique that isn't currently utilized that bases things on the weight of the various tips. (edited)

raganius (Ivan Liborio)
[12:16 AM]
Bring enough rogue IoT devices online, execute your attack, and prove your point :slightly_smiling_face:
Micah Zoltu
@limo https://iotatangle.slack.com/archives/C3V610ULS/p1497477929445557
Posted in #tanglemathToday at 12:15 AM
(edited)

Andreas Osowski [12:17 AM]
@micah.zoltu it does. the tip selection stuff.

nihilist penguin [12:17 AM]
joined #tanglemath

Kamal Mokeddem [12:17 AM]
Is the code for the COO available somewhere?

Micah Zoltu [12:17 AM]
So all you have to do to hold the network hostage is ensure that only your tips are confirmed, and your tips are the dominant tips in the network.

Tristan [12:17 AM]

So Micah can you propose a tip selection algorithm that would be better?

dylan [12:17 AM]
@raganius such an attack is not possible to simulate right now as I doubt Micah has a supercomputer or the computational means necessary able to carry out the attack. the point is that someone else with that kind of power could carry it out. that level of computational strength already exists right now, simulation of nodes is more than possible (edited)

Micah Zoltu [12:18 AM]
@tristan Better in the sense of more selfish?

raganius (Ivan Liborio)
[12:18 AM]
So (using the blockchain argument) come back when you have a supercomputer
dylan
@raganius such an attack is not possible to simulate right now as I doubt Micah has a supercomputer or the computational means necessary able to carry out the attack. the point is that someone else with that kind of power could carry it out. that level of computational strength already exists right now, simulation of nodes is more than possible
Posted in #tanglemathToday at 12:17 AM
 5 replies Last reply today at 12:23 AM View thread

Fahad Sheikh [12:18 AM]
@david @come-from-beyond there is no point publishing a white paper if it is not going to be defended. Asking for a physical manifestation is not a logical defense. Which is why many devs complain that IOTA dev just go hostile but don't give a proper argument in defense.

Alon Elmaliah [12:18 AM]
@moke , Coo is just an ordinary node - which send txs, these txs are signed w/ a key that is recognized in the current nodes. (edited)

Micah Zoltu [12:19 AM]
I don't _personally_ have the means/desire to short $1B IOTA, then buy $10M worth of hardware and hold the network hostage until IOTA price tanks. :slightly_smiling_face: (edited)

Winston [12:19 AM]
Micah's point is that there's no way of enforcing the use of a ubiquitous tip selection process. Individuals will theoretically choose the most beneficial process for their own needs over the long term
Tristan
So Micah can you propose a tip selection algorithm that would be better?
Posted in #tanglemathToday at 12:17 AM
(edited)

Micah Zoltu [12:20 AM]
:point_up: is really my primary argument. I fear that everyone using a selfish strategy will result in the network falling apart.

[12:20]
No one wins in this situation, so it isn't so much an attack as it is a slow heat-death.

[12:20]
A tragedy of the commons.

Mat
[12:21 AM]
joined #tanglemath

Kamal Mokeddem [12:21 AM]
When does the COO go away? Where is it explained why you need a COO and how long it will be around?
7 replies Last reply today at 12:26 AM View thread

Fahad Sheikh [12:22 AM]
Expected to be made optional next month. Right now its to prevent the 34% attack as the network is small.

Tristan [12:23 AM]
So if nobody wins, then isn't it the best strategy to use the suggested tip selection algo?

k_day [12:24 AM]
joined #tanglemath

Micah Zoltu [12:25 AM]
@tristan The problem is that for any _individual_ participant, the selfish strategy is optimal. Its textbook tragedy of the commons: https://en.wikipedia.org/wiki/Tragedy_of_the_commons Wikipedia
Tragedy of the commons
The tragedy of the commons is an economic theory of a situation within a shared-resource system where individual users acting independently according to their own self-interest behave contrary to the common good of all users by depleting or spoiling that resource through their collective action. The concept and name originate in an essay written in 1833 by the Victorian economist William Forster Lloyd, who used a hypothetical example of the effects of unregulated grazing on common land (then colloquially Show more… (159kB)
7 replies Last reply today at 12:49 AM View thread

raganius (Ivan Liborio)
[12:26 AM]
>I started the argument by asserting that the parent selection strategy would not be the dominant one because there are more selfish parent selection strategies available.
"The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes" NAKAMOTO. 'Bitcoin'

>what's the problem in honesty of nodes as a parameter?

>Or did I get it all wrong?

>Or maybe we should all go back to Western Union and mastercard ?

Limo Tangleblog.com
[12:26 AM]
this is really complex,

and only the big guys should talk here, but how would anyone attack the tangle if it's a big mesh net + big distributed hasrate + mutual tethering + logistical nightmare to get a majority?

raganius (Ivan Liborio)
[12:27 AM]
@micah.zoltu do the attack or lose face... sorry

Sunny Aggarwal [12:27 AM]
Sorry, another aside: I just want to publicly state for the record that on Reddit and on this channel, I am not acting as a representative of Blockchain at Berkeley. Just a private cryptocurrency enthusiast! These opinions are all my own. (edited)

raganius (Ivan Liborio)
[12:27 AM]
@sunny as well

Kamal Mokeddem [12:27 AM]
Is there any explanation of why you don't need it next month? What's stopping a 34% attack at that point? Even at 100 tx/sec it doesn't seem to be much proof of work. Nobody answered why the network doesn't become more vulnerable to attacks as it grows since it's value will be growing faster than it's proof of work hashrate.

Mat Tam [12:28 AM]
@micah.zoltu @sunnya97 Would the attack be able to be demonstrated using a small testnet? So you don't need a supercomputer, you just need a normal one attacking a much smaller testnet

Limo Tangleblog.com
[12:28 AM]
well @sunnya97 , I found it very strange that you were showing your concerns in a newby channel (on reddit) where possibly thousands of people read that, while you are a foundation connected dude, that is also my personal opinion (edited)

3 replies Last reply today at 12:44 AM View thread

Fahad Sheikh [12:29 AM]
Thats what I think too Mat. The attack should be replicable in a testnet with a small enough network that doesn't require a supercomputer but big enough that the conditions are representative.

[12:30]
I can host a node for this if needed :slightly_smiling_face:

Tristan [12:30 AM]
So @micah.zoltu you're saying by implementing a selfish strategy your transactions would be confirmed faster? Are they not fast enough? Or are you saying by implementing a selfish strategy you can take down the whole network and profit by shorting? Because that seems more malicious than just selfish

Micah Zoltu [12:31 AM]
@zero The confirmation failure could easily be replicated. Just modify IOTA code to simply only select its own parents and then create a network of nodes.

[12:31]
@tristan Yes, a selfish strategy would result in your transactions confirming faster than a non-selfish strategy.
Yes, transactions are abysmally slow right now. I want sub-second ideally, seconds is OK, minutes is unacceptable.

[12:32]
For the sake of keeping things focused, I propose we ignore any explicit profitable attacks for now. I suspect they exist and I have eluded to how they would work, but I think that is a less interesting angle to discuss than the fact that the network will simply crumble on its own over time.

Tristan [12:33 AM]
So when the network is large/active enough for second confirmations you think people will care enough to implement their own tip selection strategy to shave off a few fractions of a second?

Come-from-Beyond [12:33 AM]
@hellsingfan Just accumulate a lot of transactions and release them to the mainnet, the same effect

Fahad Sheikh [12:34 AM]
@come-from-beyond isn't the COO going to protect the network currently?

Micah Zoltu [12:34 AM]
@tristan Yes. I know I would, especially if I was building anything against IOTA.

Come-from-Beyond [12:34 AM]
well, i probably didn't get what attack is going to be tested.

[12:34]
i thought that supercomputer attack

Fahad Sheikh [12:38 AM]
Hmm... i just feel like its in everyone's interest to discuss this through.

Dominik Schiener [12:40 AM]
if given the resources, who would feel comfortable in coming up with the attack?

[12:40]
@micah.zoltu @sunnya97

[12:41]
coming up in the sense of clearly defining it for our simulations framework (potentially even help with the implementation of it)

Come-from-Beyond [12:41 AM]
> i just feel like its in everyone's interest to discuss this through.
Nay, just push the txs, below 126 TPS was already tested and above is interesting to test especially if we don't need to pay for spamming)

[12:41]

in the worst case only few edge nodes will die

Tim Calahan [12:42 AM]
joined #tanglemath

Micah Zoltu [12:42 AM]
@dom The gist would be to create an IOTA client where each node _only_ selects its own transactions as parents and spams the network. Then create a network full of such clients and see how things work out.

Dominik Schiener [12:43 AM]
I don't need a gist

[12:43]
I'm giving you the opportunity to work with a team of students and the resources you need (as described above) to come up with an attack

Fahad Sheikh [12:43 AM]
@come-from-beyond can't the argument be defeated logically that one must resort to the a physical implementation? That just means the white paper needs a lot of work, if true.

Dominik Schiener [12:43 AM]
it'll probably make it into our whitepaper 2.0

Come-from-Beyond [12:44 AM]
@hellsingfan I didn't get your thought

Kamal Mokeddem [12:44 AM]
@dom I had the exact same thought as micah after reading the white paper.

Dominik Schiener [12:45 AM]
great, then lets do it

Max Reimann [12:45 AM]
joined #tanglemath

Come-from-Beyond [12:45 AM]
Has anyone saved the convo above? I wouldn't need to explain nuances of IoT again...

[12:45]
I can't fetch it without crashing Slack app

Micah Zoltu [12:45 AM]
@dom Ah, I have _way_ too many projects on my plate right now to get involved in another one, especially if I am starting with the point of view that the system is unsound and looking to convince myself otherwise.

Winston [12:45 AM]
Saved @come-from-beyond

Come-from-Beyond [12:46 AM]

great

Dominik Schiener [12:46 AM]
find another skeptic and we'll hire him for consultancy or whatever

Micah Zoltu [12:46 AM]
Sounds like there are a few in here, perhaps one is interested. :slightly_smiling_face:

Fahad Sheikh [12:46 AM]
@sunnya97 why don't you do it given you're attached to the Foundation as well and have been arguing as well.

Kamal Mokeddem [12:47 AM]
I'm not, I came here to invest if I could satisfy myself that the tech is sound, starting with security of course.

Micah Zoltu [12:47 AM]
Though, the definition of the "attack" is simply:
* every node selects its own transactions as parents only.

[12:47]
There really isn't anything more to it than that.

Dominik Schiener [12:47 AM]
@alon.elmaliah what do you think?

[12:48]
> There really isn't anything more to it than that.

need one of you to read and understand the code and greenlight it as well as the results

[12:48]
especially when it comes to running the simulations there is more work involved

Alon Elmaliah [12:49 AM]
I think it's a great idea - would love it if one of you guys join me in implementing the attack on the simulation framework.

Fahad Sheikh [12:49 AM]
@micah.zoltu and the expected result of that is?

Micah Zoltu [12:49 AM]
@hellsingfan Confirmation never occurs.

Dominik Schiener [12:50 AM]
@alon.elmaliah I'm starting to think that for the simulations we should have a public website where people can submit ideas / concerns / attacks

Alon Elmaliah [12:50 AM]

>* every node selects its own transactions as parents only.
that's a dead-lock by design
I think we can think of a more sophisticated attack - that changes state over time. (edited)

Micah Zoltu [12:50 AM]
You effectively end up with a bunch of sub-tangles and no main tangle (or perhaps a single main tangle).

Dominik Schiener [12:50 AM]
those are then ranked and the most upvoted ones get implemented and tested (edited)

Micah Zoltu [12:50 AM]
@alon.elmaliah Yeah, exactly. But that is where things end up if actors behave selfishly.

[12:50]
Avoiding the deadlock requires a significant amount of network resources (hashpower) to behave altruistically.

Alon Elmaliah [12:50 AM]
yes - but that is also a falicy - you need to transition to that. you can't just assume they all start off selfish. no point in testing that imo. (edited)

Paul H [12:51 AM]
If you're selfish and knowingly create a subtangle that will not merge and confirm, what is the benifit?

Sunny Aggarwal [12:51 AM]
I have a full-time internship that takes up a lot of my time. However, I guess I can put in some time to try to help with a simulation. I'm going to need some help though cause I've never done something like this before haha (edited)

Micah Zoltu [12:51 AM]
The transition is simple. Someone releases a client that gives you faster confirmation times than the reference implementation. Over time, people adopt it because it is better for _them_.

Dominik Schiener [12:51 AM]
full time internship at Consensys, hmm

Micah Zoltu [12:52 AM]
@paulh Because you get faster confirmation times. (edited)

Paul H [12:52 AM]
do you?

Fahad Sheikh [12:52 AM]
@micah.zoltu how is it better for them when confirmation never happens?

Paul H [12:52 AM]
you take a risk of not being confirmed

[12:52]
for a lot of work

Micah Zoltu [12:52 AM]
I believe so because you effectively "promote" your own transactions in terms of liklihood of being picked by altruistic nodes.

Paul H [12:52 AM]
ok, so you end up keeping a cohesive tangle

Micah Zoltu [12:53 AM]
@hellsingfan It is better for each individual right up until the network deadlocks.

Paul H [12:53 AM]
what's the problem then?

[12:53]
I thought the assumption was mostly selfish, so which is it?

[12:53]
what percentage must be selfish

[12:53]
such that the network irreparably breaks?

Micah Zoltu [12:53 AM]
So there are 3 states:
1. everyone is altruistic
2. some are altruistic, some are selfish
3. enough are selfish to deadlock the system

Fahad Sheikh [12:53 AM]
@micah.zoltu and then you end up transitioning back to a state that is beneficial. Thats essentially how we have 'civilized societies' and not rule of the jungle.

Paul
H [12:54 AM]
1) no problem here

[12:54]
2) need evidence* of a problem here (edited)

Micah Zoltu [12:54 AM]
@hellsingfan It isn't a healthy equilibrium to have the system being in a perpetual state of deadlocked => not deadlocked => deadlocked (which is the equilibrium).

[12:55]
2 isn't a problem, it is the path to the problem.

Paul H [12:55 AM]
3) don't see the winning stategy here (who wins the game?) (edited)

Micah Zoltu [12:55 AM]

No one "wins".

[12:55]
The network dies.

[12:55]
It can be resurrected, but then it dies again.

Paul H [12:55 AM]
ok

Kamal Mokeddem [12:55 AM]
is it not obvious that an attacker with enough hashpower could selfishly select tips such that no real transactions confirm (once COO no longer exists)?

Micah Zoltu [12:55 AM]
You can keep resurrecting it and letting it die again, but the equilibrium is at the edge of death.

Fahad Sheikh [12:55 AM]
The end game of your attack would leave the network unusable for the attacker themselves. Which means the 'selfish' strategy is actually not to be selfish.

Micah Zoltu [12:56 AM]
Its not an "attack". It is a natural state.

Paul H [12:56 AM]
so we have a periodic shit the bed, restore, shit the bed, restore

Micah Zoltu [12:56 AM]
No one is malicious in this scenario, they are selfish.

Paul H [12:56 AM]
is that right?

[12:56]
of course

Micah Zoltu [12:56 AM]
Yes.

Paul H [12:56 AM]
ok

[12:56]
so if I'm selfish

[12:56]
I'm taking the risk that I shit the bed for everyone and have to do it all over again

Serguei Popov [12:56 AM]
OK, let me see what we have here...

Micah Zoltu [12:57 AM]
Only if you are the straw that breaks the system.

Paul H [12:57 AM]
What's the threshold, then?

Micah Zoltu [12:57 AM]
It is beneficial to be selfish right up until the system breaks under the pressure of everyone being selfish.

[12:57]
Not sure the exact threshold, haven't bothered to work out the numbers.

[12:58]
https://en.wikipedia.org/wiki/Chicken_(game) (edited)

[12:58]
Related, though not a perfect fit.

Fahad Sheikh [12:58 AM]
Basically you're saying the system is breakable. BUT to not be selfish is actually better for the bad actor themselves. I feel like the equilibrium will shift towards not being as selfish. The system will transition back to the healthy state and then you will not find enough bad actors to transition to the unusable state.

Ike spear [12:58 AM]
joined #tanglemath

Paul H [12:58 AM]
Yeah, chicken is a game of two, no? (edited)

Micah Zoltu [12:58 AM]
Hawk-dove isn't, which is what I was referring to.

Paul H [12:59 AM]
We should probably slow down so @mthcl can read up

[12:59]
but I have a lot of caffeine in my blood right now

Fahad Sheikh [12:59 AM]
lol

Micah Zoltu [12:59 AM]
@hellsingfan No, being selfish is the optimal strategy for any individual at any point in time with the exception of the point in time which the system deadlocks.

Paul H [12:59 AM]
Of course being selfish is optimal

[12:59]

but what percentage of selfishness helps me best?

Micah Zoltu [12:59 AM]
There is a single instantaneous point where it is _not_ in the best interest of a party to be selfish because their being selfish breaks the entire network.

Fahad Sheikh [1:00 AM]
Does this selfish entity have memory? Thats why I gave the example of civilized societies.

Micah Zoltu [1:00 AM]
Because the network cannot react fast enough to this, the network gets into a pathological state of deadlock-recover-deadlock-recover which is _super_ unhealthy.

Paul H [1:00 AM]
I'm trying to keep pace here, but feeling jittery

Fahad Sheikh [1:00 AM]
We're not going back to barbaric times even if those might be optimal for an individual. And certainly won't convince majority to follow suit.

Micah Zoltu [1:01 AM]
If IOTA _depends_ on people acting non-selfishly "for the greater good" then most of my arguments go away.

[1:01]
I do not think that is a healthy assumption in a pseudoanonymous world though.

Kamal Mokeddem [1:01 AM]
What about a dedicated attacker? Is it not obvious that an attacker with enough hashpower could selfishly select tips such that no real transactions confirm (once COO no longer exists)?

Micah Zoltu [1:02 AM]
Especially since someone could force the deadlock maliciously and short IOTA or hold it hostage at profit (which _is_ an attack, but again I want to focus on just the natural death of the system).

[1:02]
@moke I believe so, yes.

Paul H [1:02 AM]
Do you want to go there now, @moke ?

Fahad Sheikh [1:02 AM]
Well in my opinion the equilibrium will shift. But to your point though the system should not be breakable to begin with. @paulh can't there be a safeguard put in place?

Paul H [1:02 AM]
Shelve selfish for the moment?

Kamal Mokeddem [1:02 AM]
yes

Paul H [1:02 AM]

k

[1:03]
So what does the attacker stand to gain?

[1:03]
Free transmission of his virus?

Kamal Mokeddem [1:03 AM]
the death of the network?

Sunny Aggarwal [1:03 AM]
Yeah, exactly. If everyone just worked in the greater good, we probably wouldn't need blockchains in general. The whole point was to be game theoretically secure

Paul H [1:04 AM]
I think this is too complex to discuss all scenarios all at once

[1:04]
I haven't had enough sleep in the last month to handle that, at least.

Kamal Mokeddem [1:04 AM]
let's discuss dedicated attacker

Micah Zoltu [1:04 AM]
@paulh The immediately obvious attack to me is shorting IOTA then breaking the network. There may be better attacks.

Kamal Mokeddem [1:05 AM]
agreed

Paul H [1:05 AM]
Ok

[1:05]
So we assume the attack is a short?

Kamal Mokeddem [1:05 AM]
double spend is obvious extension of that

Micah Zoltu [1:05 AM]
Double spends would potentially be more lucrative if you could do enough volume before anyone noticed. Though I'm not sure on the specifics enough to know exactly how to execute that in the face of selfish participants.

Paul H [1:06 AM]
sure, great. shall we assume a double spend, or malicious attack?

[1:06]
which to tackle first?

[1:06]

we could make a list

Kamal Mokeddem [1:06 AM]
denial of service is basic

[1:06]
so start there

Paul H [1:06 AM]
which?

[1:06]
dos?

Kamal Mokeddem [1:06 AM]
yes

Micah Zoltu [1:06 AM]
Off the top of my head, to double spend you would leverage the selfish participants to reduce the hashing power required to attack the network.

[1:06]
I don't have a full double spend modeled, so I agree... DoS + short is easier.

Paul H [1:06 AM]
ok, for DoS to work, you have to be doing more, higher work than people who just want their transactions to go through

[1:07]
and you have to fill up broadcast buffers

Micah Zoltu [1:07 AM]
And again I want to be crystal clear: I have not fully thought through the attack vector! The equilibrium of failure was where I stopped, attacks can _likely_ be built on top of it.

Paul H [1:07 AM]
well,

[1:07]
I've had enough coffee to help you thing it through

[1:07]
and I went on a run

[1:07]
so I'm well oxygenated

Micah Zoltu [1:07 AM]
@paulh You have to be doing more work than the _altruistic parties_.

[1:08]
The selfish parties aren't helping to secure the network, they are helping themselves.

Paul H [1:08 AM]
what?

Kamal Mokeddem [1:08 AM]
why do you have to fill up the broadcast buffers? I'm talking about denial of service where you are doing more work than the altruistic network

Paul H [1:08 AM]
Are we not talking about DoS anymore?

Tim Calahan [1:08 AM]
So IOTA reference client uses a tip selection algorithm that is good for the network, but selfish strategy could be used to prevent others to confirm their tx's?

Paul H [1:08 AM]
maybe I didn't get enough coffee

Micah Zoltu [1:08 AM]
Its a DoS in the sense that it brings the network to a deadlock. Not in the sense of filling up network buffers.

Paul H [1:08 AM]
It includes a selfish option

Kamal Mokeddem [1:08 AM]
denail of service in the sense that altruistic transactions do not confirm

Paul H [1:08 AM]
shameless self promotion of tx

Kamal Mokeddem [1:09 AM]
yes

Paul H [1:09 AM]
(at least v1.2 does)

[1:09]
but it's only half-selfish so that you don't risk getting left out)

Tim Calahan [1:09 AM]
I may have a solution for the selfish strategy problem. Is there a bounty? :slightly_smiling_face:

Micah Zoltu [1:09 AM]
You basically select parents such that all of your transactions are always bubbling up to the top so they are selected by altruistic parties. You do not choose _anyone else_ as a parent.

Kamal Mokeddem [1:10 AM]
exactly

Paul H [1:10 AM]
@dom @timcalahan seems to volunteer!

[1:10]
Tim, if you'd like to volunteer, you can of course get a bounty

Micah Zoltu [1:10 AM]
Altruistic people are doing a form of semi-random selection, and they will tend to pick selfish transactions over non-selfish ones, but they won't be included in any selfish party's transaction.

Paul H [1:10 AM]
I'd hope that you familiarize yourself with the code first, though

Sunny Aggarwal [1:10 AM]
@timcalahan I think @david and @dom implied that if we prove a problem exists, there's a bounty available, so I'm sure there's definitely a bounty if you provide a solution too!

Micah Zoltu [1:10 AM]
So with enough selfish parties, you end up with a bunch of sub-tangles and no confirmation.

Alon Elmaliah [1:11 AM]
@timcalahan -- read dom's posts above. if you can find them :slightly_smiling_face:

Tim Calahan [1:11 AM]
My idea is so simple, that it can be explained in one sentence. It could be wrong, and most likely is.

Paul H [1:11 AM]
@micah.zoltu are we done discussing DoS?

[1:11]
DoS has less to do with tip selection in iota

[1:11]
more to do with network packet flooding

[1:11]
unless you can enlighten me otherwise

Micah Zoltu [1:12 AM]
I was never discussing a DoS in that sense.

Kamal Mokeddem [1:12 AM]
neither was I

Sunny Aggarwal [1:12 AM]
@paul I think
we were using different meanings of Dos.

Paul H [1:12 AM]
let's pin something down

[1:12]

it's too boring for me to talk in vague terms

Tim Calahan [1:12 AM]
Ok, the crude idea of my tip selection algo / protocol rule is this:
The hash of the two tx's selected to be confirmed has to follow the rule: XOR'ing them must produce a hash that satiesfies some rule, such as certain number of leading zeros in it. The optimal rule could be found by simulation or math.
+1 32 replies Last reply today at 1:43 AM View thread

Micah Zoltu [1:12 AM]
I believe @moke @sunnya97 and I are all on the same page with the strategy I just described.

Sunny Aggarwal [1:12 AM]
Alright everyone pause typing for a second.

Fahad Sheikh [1:13 AM]
@micah.zoltu if the tip selection method is forced to be the same as what IOTA uses currently. Does the attack seize to exist.

Sunny Aggarwal [1:13 AM]
Let @micah.zoltu describe the DoS we're talking about so we can all be on the same page (I'm on my phone atm) (edited)

Kamal Mokeddem [1:13 AM]
the attack is that altruistic transactions never confirm. We are calling that denial of service, because that is what it is. the network would be unusable.

Micah Zoltu [1:15 AM]
* Selfish client spams network with transactions. These transactions have parents that are transactions this actor _wants_ promoted. They never promote anything that doesn't benefit them.
* Altruistic actors will randomly select parents (or MCMC or whatever).
* Given enough selfish actors, you end up with a situation where there are a bunch of heavy weight sub-tangles (which matters for confirmation) that include almost nothing else except the selfish actor's own transactions (and transactions where someone else sends them something).
* The altruistic actors are constantly _trying_ to merge sub-tangles but they don't have enough weight to make it stick (confirm). (edited)

Alon Elmaliah [1:15 AM]
(and give @mthcl some ~time~ space to respond :slightly_smiling_face:) (edited)

Kamal Mokeddem [1:17 AM]
The fact that it's not obvious what the attack would be is concerning in and of itself. I have to go.

Paul H [1:18 AM]
It's concerning that there's not a clear definition of a successful attack?

Micah Zoltu [1:18 AM]
The above describes how the network can die a natural death.

[1:18]
A malicious actor can throw computing resources at the problem to bring the above about faster.

[1:19]
A malicious actor is _helped_ by selfish actors (who don't even have to know an attack is happening).

Alon Elmaliah [1:19 AM]
>>>* Given enough selfish actors, you end up with a situation where there are a bunch of heavy weight sub-tangles (which matters for confirmation) that include almost nothing else except the selfish actor's own transactions (and transactions where someone else sends them something). (edited)

[1:19]
you need to touch base every once in while (connect to honest subtangle) - if not the MCMC won't even see you, this would make the selfish actor approve honest txs as well. (edited)

Micah Zoltu [1:19 AM]
And as @sunnya97 mentioned earlier, the altruistic actors only defend when they are actively doing PoW. Any participant who only hashes when they have a transaction is only contributing to security for the time they are hashing.

Paul H [1:20 AM]
So what are the assumptions of the selfish issuer of transactions?

Micah Zoltu [1:20 AM]
@alon.elmaliah The MCMC (I believe) is the parent selection strategy, not confirmation strategy.

Paul H [1:20 AM]
yes

Alon Elmaliah [1:20 AM]
I meant the selection - it dosent start at genesis, it starts at some depth back. (edited)

Micah Zoltu [1:20 AM]
Also, you are constantly issuing transactions, so you always have recentr transactions available to be built on. (edited)

[1:21]
@paulh The selfish actor is simply selecting parents that he actively wants promoted. He never selects a parent that he doesn't actively care about.

Sunny Aggarwal [1:21 AM]
@paulh Some potential attacks involving DoS:
- Temporary DoS in order to short the market
- Long term DoS in order to hold the Tangle Hostage (in order to start charging fees perhaps)
A separate type of attack:
- Double spend attacks (needs a lot of hash power but it is *far* easier to do this in a Tangle than in a blockchain) (edited)

Alon Elmaliah [1:22 AM]
sunny, could you describe a DS attack?

David Sønstebø [1:22 AM]

how is a DS attack *far* easier / cheaper in a Tangle vs a Blockchain?

Micah Zoltu [1:22 AM]
Because most participants are only hashing when they want to transact. Time spent idle is time spent _not_ securing the network.

[1:23]
There is no incentive (block rewards/transaction fees) for a selfish but honest participant to secure the network by hashing during idle time.

David Sønstebø [1:24 AM]
I don't think you guys quite grasp the full vision of IOTA. IOTA enables *streams* of transactions (due to no fees)

[1:24]
IOTA came about *after* considering the hardware environment, not the other way aound

[1:24]
IOTA exist soley due to hardware

Micah Zoltu [1:25 AM]
As long as the confirmation algorithm is based on proof of work, someone can dedicate computing resources to doing more of that.

[1:26]
If the confirmation algorithm is not based on proof of work, then someone can dedicate computing resources to a Sybil attack (lots of simulated nodes).

David Sønstebø [1:26 AM]
So you presume someone will spend 50K to double spend 10 cents?

Micah Zoltu [1:26 AM]
No, but to doublespend $1M. Yes.

David Sønstebø [1:26 AM]
why would you send $1M in a singular transaction?

[1:26]
why not simple chop it into $1 chunks?

Micah Zoltu [1:26 AM]
Then double spend those chunks.

Sunny Aggarwal [1:27 AM]
Because then you have to do 1000000x the PoW

David Sønstebø [1:27 AM]
then you lose money again...

Micah Zoltu [1:27 AM]
Heh, that too. :slightly_smiling_face:

David Sønstebø [1:27 AM]
from a game theoretic POV, is your argument that the actor is irrational?

Micah Zoltu [1:27 AM]
No, they are rational.

David Sønstebø [1:27 AM]
Losing orders of magnitude doesn't sound rational

Micah Zoltu [1:27 AM]
No one is losing orders of magnitude here.

Sunny Aggarwal [1:28 AM]
Consider that some attacks might also seem irrational from the perspective of the network but are in fact rational when considering external factors

[1:28]
Such as shorting the market

David Sønstebø [1:29 AM]
This is basic, your postulate is that someone shorts, assumes that their 'attack' will result in a profitable gain, and that the attack will cost less than the attack, right?

Micah Zoltu [1:29 AM]
I go to two different exchanges. I initiate a transfer to one for $1M worth of IOTA. Once it confirms I then attack the network to double-spend by sending $1M worth of IOTA to a _different_ exchange. This is standard double-spend attack.

[1:29]
(again, I don't know why people keep gravitating toward double spend though, I think the natural death is more interesting, easier to discuss, more fleshed out, and harder to fix)

David Sønstebø [1:30 AM]
How would you be able to double spend with only $1m?

[1:30]
'antural death' = elaborate

[1:30]
natural*

Micah Zoltu [1:30 AM]
https://iotatangle.slack.com/archives/C3V610ULS/p1497482145287991
Micah Zoltu
* Selfish client spams network with transactions. These transactions have parents that are transactions this actor _wants_ promoted. They never promote anything that doesn't benefit them.
* Altruistic actors will randomly select parents (or MCMC or whatever).
* Given enough selfish actors, you end up with a situation where there are a bunch of heavy weight sub-tangles (which matters for confirmation) that include almost nothing else except the selfish actor's own transactions (and transactions Show more…

Posted in #tanglemathToday at 1:15 AM

[1:31]
Describes the deadlock, where selfish actors have all created separate subtangles that never confirm.

[1:31]
Alternatively, _one_ of the subtangles confirms and that participant now controls the network (no one else can get into his subtangle).

David Sønstebø [1:31 AM]
Did you calculate in cost of setting up these selfish actors?

Micah Zoltu [1:31 AM]
Its basically PoW computing costs and bandwidth costs in the long-run. (edited)

[1:32]
R&D costs should be dwarfed by those if you plan things out well.

David Sønstebø [1:32 AM]
Sure, but lets presume a post-Coo era. VS 1 million 'honest actors' how much do you think it will cost to gain even a remotely relevant stake in the network?

Micah Zoltu [1:33 AM]
Not much if those 1M are only hashing when they transact.

[1:33]
And at the moment, remember that there are $1.5B on the line (though, would require you find someone to take on your short of $1.5B). (edited)

Sunny Aggarwal [1:34 AM]
A remotely relevant share of computational power or share of the currency? (edited)

Micah Zoltu [1:34 AM]
More likely you would short on a futures market with massive leverage.

David Sønstebø [1:35 AM]
I feel that neither of you realize that IOTA is meant to be a continuously streaming network of *MICRO* transactions

[1:35]
If you want to transact a million dollar you do that in a stream of 1 million 1 dollar tx, not one 1 mio tx

[1:35]
this is the beauty of IOTA

dylan [1:36 AM]
there is a hard cap on how much you can send?

David Sønstebø [1:36 AM]
no

[1:36]
it's all probabilistic

[1:36]
this is true for blockchain as well

Micah Zoltu [1:36 AM]
1. Unless there is a cap you can't control _how_ people use the network.
2. Even if you stream the transactions, you either have to wait for each to confirm before moving on to the next or you have to treat the stream as a single transaction for the sake of security.

David Sønstebø [1:36 AM]
If I send you 50 cent you might accept it after 50% of the network reference it, but if I send you 1 million you might
want to wait until 99% does

[1:37]
these are heuristics, nothing about the core protocol

Micah Zoltu [1:37 AM]
Right. Which means if people are using the selfish strategy the $1M will never "confirm".

David Sønstebø [1:38 AM]
Micah: if I offer you 10K to demontrate this, will you do it tomorrow?

Sunny Aggarwal [1:38 AM]
That 99% might never happen though because of the subtangles not converging though?

Micah Zoltu [1:38 AM]
And 2M transactions of $0.50 each will similarly never complete because the system _never_ reaches 99% confirmation.

[1:38]
@david As I have said many times, I am _way_ too busy to go and engineer a solution to your problem. I came here trying to be helpful, not to actively attack your network.

[1:39]
If I am going to engineer something it will be an _actual_ attack against the network because that is worth way more than $10k.

David Sønstebø [1:39 AM]
@micah.zoltu so essentially 10K is 'nothing to you', you want to be a malevolent actor and earn more? Ok, I am looking forward to it now that you admitted you're looking for a bigger pay out

Alon Elmaliah [1:39 AM]
(I want to ask you guys to take a second to process the concepts david is raising, these aren't trivial - take a sec to let them sink before replying :slightly_smiling_face:) (edited)

Micah Zoltu [1:40 AM]
@david 1) yes, 10k is definitely not worth the effort required to me. 2) I was trying to be helpful by bringing up concerns with the game theory proposed in the whitepaper.

Serguei Popov [1:40 AM]
Guys, you write faster than I read!!!

David Sønstebø [1:41 AM]
How much would it cost for you to prove this attack @micah.zoltu ?

Micah Zoltu [1:41 AM]
@alon.elmaliah Unfortunately, he is saying the same thing that those before him have been saying. It is unclear why either we are unable to see their argument or they are unable to see our argument. I feel like one of the two groups is _completely_ missing something intrinsic that the other group assumes.

David Sønstebø [1:41 AM]
I live in Norway and think "damn, 10K for an evening's work? yesplx", you must be living on mars with those prices

Micah Zoltu [1:42 AM]
I have been an engineer long enough to know that authoring an attack against a foreign system is not "a days work". (edited)

[1:42]
I believe @come-from-beyond was driving at it with his underlying belief of a global web of trust, but he never did explain how he intended to build that.

Alon Elmaliah [1:43 AM]
@micah.zoltu if you think so, then at least help @mthcl to catch up..

David Sønstebø [1:44 AM]
As I have said 100 times, we *Welcome* these kind of discussions and attacks, this is what new experimental tech is all about, but for some reason it always ends at these speculative discussions. In the past 1.5 years not a single attack has occured successfully

[1:44]
even with millions on the line

Micah Zoltu [1:45 AM]
You have the COO.

[1:45]
The COO _is_ a defense against almost any attack.

David Sønstebø [1:45 AM]
Not any attack, Coo is simply like training wheels

[1:45]
If you truly found a flaw in Tangle itself it should be quie easy to pove

[1:45]
prove*

Micah Zoltu [1:45 AM]

COO is a proof of authority model. _vastly_ different from a decentralized system.

Fahad Sheikh [1:45 AM]
Can we do this on the testnet? You don't need a supercomputer for that :wink:

Micah Zoltu [1:46 AM]
@hellsingfan Possibly, but that wouldn't be profitable for an attacker.

David Sønstebø [1:46 AM]
Tell me what you want then

[1:46]
We can give you nodes, supercomputers

Fahad Sheikh [1:46 AM]
we're not asking for anyone to profit. We're seeing if the attack is possible.

David Sønstebø [1:46 AM]
just specify the parameters

Micah Zoltu [1:46 AM]
_I_ don't want anything in particular. I was just trying to be helpful by sharing a flaw in the login of the whitepaper.

Fahad Sheikh [1:47 AM]
So just execute the attack on testnet.

David Sønstebø [1:47 AM]
@mthcl do you feel that the whitepaper has been invalidated by this discussion?

Fahad Sheikh [1:47 AM]
If it can be done in testnet, it can be done on main net through a supercomputer. Point proven.

Serguei Popov [1:47 AM]
No.

Micah Zoltu [1:47 AM]
@hellsingfan Not sure how many different ways I can say that I don't have the time nor inclination to go build an attack against the system for free, or even for $10,000.

Serguei Popov [1:47 AM]
>Micah Zoltu 4:06 PM
>Up until that point, it seemed that the conclusion that was being arrived at is that Iota
>equilibrium requires the majority of participants behaving in a way that is "good for the network" rather than in a way that is purely selfish.

Not true. Please, speak for yourself.

>Micah Zoltu
>4:40 PM
>I don't believe it matters since I believe this strategy is better (from a selfish perspective),

>over time everyone save for the altruistic participants will migrate towards it.
>By selecting your own transactions as parents, you increase the chances that someone else
>will pick you as their parent using one of the random selection strategies.

I doubt that "selecting your own transactions as parents" is a good strategy even for a "completely selfish" (whatever it means) node. Because
(1) other selfish nodes won't reference your transactions because they owe nothing to you;
(2) "honest" nodes won't reference your transactions because the random walk is very unlikely to choose them (see the "lazy tips" on figure 6 in the whitepaper).
Therefore, if your goal is to get your transaction confirmed by the network, you should better do something that would cause at least the honest nodes to reference it

[1:48]
>Micah Zoltu
>7:47 PM
>Though, the definition of the "attack" is simply:
>* every node selects its own transactions as parents only.

As mentioned above, this is, well... not a _clever_ idea :slightly_smiling_face:

>Micah Zoltu
>7:56 PM
>Its not an "attack". It is a natural state.

Think again of the above toy model.

>Micah Zoltu 8:15 PM
>* Selfish client spams network with transactions. These transactions have parents that are transactions this actor wants promoted.
> They never promote anything that doesn't benefit them.
>* Altruistic actors will randomly select parents (or MCMC or whatever).
>* Given enough selfish actors, you end up with a situation where there are a bunch of heavy weight sub-tangles
>(which matters for confirmation) that include almost nothing else except the selfish actor's own transactions
>(and transactions where someone else sends them something).
>* The altruistic actors are constantly trying to merge sub-tangles but they don't have enough weight to make it stick (confirm).

No! What will happen, is that the "altruistic" actors will build "their" subtangle, and all these "selfish" guys will selfishly fall to limbo.

[1:48]
Ah, and a concluding remark. Of course, it would be _nice_ to have a _proof_ that iota is secure. Believe me, I would _really_ like to be able to obtain it. But I couldn't. Well, sometimes things get too complicated. So, all I have for now is my Markov chains' intuition, about which I humbly think it deserves some respect. Besides, do you realise that _the_ _entire_ modern public-key cryptography relies on unproven assumptions?! Should we stop using it until they prove that P≠NP?

Micah Zoltu [1:48 AM]
> other selfish nodes won't reference your transactions because they owe nothing to you

@mthcl Can you explain why you believe this is the case? What would cause someone to not select me as a parent?

Andreas Osowski [1:49 AM]
because they're just as selfish as you?

Micah Zoltu [1:49 AM]
That is the world I have proposed, yes.

Sunny Aggarwal [1:50 AM]
^where everything breaks into subtangles

Serguei Popov [1:50 AM]
>Come-from-Beyond
>4:41 PM
>We assume that 67% of nodes stick to one of the good strategies.

Don't think this assumption is necessary (I don't believe in "magic numbers"). Rather, the assumption is that "a good proportion of nodes follows a 'canonical' strategy", which is a perfectly reasonable assumption in the IoT environment, at least in the beginning.

>Micah Zoltu
>7:05 PM
>The whitepaper describes a particular parent selection strategy and then defends a number of attacks based on that assumption.
>I started the argument by asserting that the parent selection strategy would not be the
>dominant one because there are more selfish parent selection strategies available.

So far, you didn't present any particular strategy that gives a significant gain to its user.

>Fahad Sheikh
>7:18 PM
>@david @come-from-beyond there is no point publishing a white paper if it is not going to be defended.

Sure, I'm usually able to defend my papers :smile:

> Tristan
>So Micah can you propose a tip selection algorithm that would be better?
>Posted in #tanglemathToday at 7:17 PM
>Micah Zoltu
>7:20 PM
>:point_up: is really my primary argument. I fear that everyone using a selfish strategy will result in the network falling apart.
>7:20
>No one wins in this situation, so it isn't so much an attack as it is a slow heat-death.
>7:20
>A tragedy of the commons.

At this point, I feel that some people try to apply intuition from Game Theory 101 to our situation, when quite a lot of (approximately) independent actors interact. Yes, it is true that, in general, if a system has unique stable state, it eventually gets there, and there remains. However, the time until it happens can be _really_ large; things of this kinds are called _metastability_ in the literature. Let us maybe consider a simple toy model. Assume that there are 100 nodes whose states can be 0 or 1; initially, there are 37 nodes in state 1, and 63 nodes in state 0. Then, at each (discrete) moment of time each node randomly chooses 50 other nodes, and
(1) if at least one of these nodes is in state 1, then the state of our node will be 1 with probability 0.8 and 0 with probability 0.2, independently of the others;
(2) if all these nodes are in state 0, then our node also becomes 0.

This is an example of a metastable situation. The only stable state is obviously "all zeros". _Eventually_, it _will_ be reached (after all, the state space of the system is finite). However, the time until it happens will be _really_ huge. I'm too lazy to do the calculations, but I'm quite sure it will be much bigger than the lifetime of the Universe... Please, think about this example. That "slow heat-death" can be _really_ slow :slightly_smiling_face:

Micah Zoltu [1:51 AM]
> "honest" nodes won't reference your transactions because the random walk is very unlikely to choose them (see the "lazy tips" on figure 6 in the whitepaper).
Based on my understanding of the whitepaper, "honest" nodes randomly choose `n` transactions from some time-window in the past and then walk randomly until they reach a tip. Then the tips of the 2 shortest paths are selected as parents.

[1:51]
Lets focus on this since all of your other arguments are based on it, and this is the part that I don't _currently_ agree with and _want_ to be convinced of.

[1:52]
You are asserting that random selection _is_ the selfish strategy. Based on the whitepaper (and all prior discussions here) I am unconvinced of this assertion and I would _really_ like to focus on that.

Serguei Popov [1:52 AM]
>@mthcl Can you explain why you believe this is the case? What would cause someone to not select me as a parent?

[1:52]
Because you'll reference tx's that are deep inside the tangle, and the RW's transition probabilities are chosen in such a way that it is extremely unlikely that the walker jumps from "deep inside" directly to a tip.

Micah Zoltu [1:53 AM]
My selfish node would be selecting its own transactions that were in the time window targeted by the honest strategy.

[1:53]
And since I am _constantly_ generating transactions, there is always plenty to choose from.

[1:54]
The selfish actor can generate a wide tangle, a narrow tangle, a long tangle, whatever. They can make it as complex/simple as they like, they are the architect.

Sunny Aggarwal [1:55 AM]
I'm heading out for dinner with a friend, so gonna be partially signing off for a bit.

Serguei Popov [1:55 AM]
> My selfish node would be selecting its own transactions that were in the time window targeted by the honest strategy.

[1:55]
But honest nodes won't select them. Your goal, I assume, is not build your own subtangle (which you can do if you want), but rather have your tx's confirmed by others. Correct?

Sunny Aggarwal [1:56 AM]
@david Can you point me in the right direction to where I can find the tools to test a simulation? If I get some time to get around to it, I'll give it a shot.

Serguei Popov [1:55 AM]
> My selfish node would be selecting its own transactions that were in the time window targeted by the honest strategy.

[1:55]
But honest nodes won't select them. Your goal, I assume, is not build your own subtangle (which you can do if you want), but rather have your tx's confirmed by others. Correct?

Sunny Aggarwal [1:56 AM]
@david Can you point me in the right direction to where I can find the tools to test a simulation? If I get some time to get around to it, I'll give it a shot.

Alon Elmaliah [1:57 AM]
(@sunnya97 - DM'd you re: simulations.) (edited)

Micah Zoltu [1:57 AM]
> honest nodes won't select them
@mthcl Why not?

[1:58]
If your answer is, "because the random walk is very unlikely to choose them" then see https://iotatangle.slack.com/archives/C3V610ULS/p1497484280644356
Micah Zoltu
> "honest" nodes won't reference your transactions because the random walk is very unlikely to choose them (see the "lazy tips" on figure 6 in the whitepaper).
Based on my understanding of the whitepaper, "honest" nodes randomly choose `n` transactions from some time-window in the past and then walk randomly until they reach a tip. Then the tips of the 2 shortest paths are selected as parents.
Posted in #tanglemathToday at 1:51 AM

Serguei Popov [1:58 AM]
because we're assuming that you cannot outperform all the others in the number of tx's (this answers why they won't be chosen as a starting point of the walk. Or did you mean smth else?) (edited)

Micah Zoltu [1:59 AM]
Why do I need to outperform all others in number of transactions to be selected?

[1:59]
Remember, we are talking about parent selection, not confirmation.

David Sønstebø [2:00 AM]
@sunnya97 we can certainly set this up, but first I want you to defend the statements you have made public. You have had a direct line to the founders of this technology, yet you've gone public with postulates about the technology and statements that are purely fallicious
14 replies Last reply today at 2:18 AM View thread

Serguei Popov [2:01 AM]
>Why do I need to outperform all others in number of transactions to be selected?
(edited)

[2:01]
Are we talking about the selection of the starting point for the walk? Or its final point?

Micah Zoltu [2:01 AM]
@mthcl Does my above description of the honest behavior for random selection not align with reality/your view?

[2:02]
https://iotatangle.slack.com/archives/C3V610ULS/p1497484280644356 is how I understand "honest" parent selection to work. Is this incorrect?

Serguei Popov [2:02 AM]
Correct. So?

[2:03]
Wait, are you thinking that the random walk is _likely_ to choose a shorter path???

Micah Zoltu [2:03 AM]
That is how I understand it from the whitepaper, yes.

Serguei Popov [2:04 AM]
Well, in fact, it's precisely the opposite.

[2:04]
The walk will "prefer" a _longer_ path towards the tips.

Micah Zoltu [2:06 AM]
OK, so selection algorithm then is:
1. randomly choose `n` nodes that are timestamped between `x` and `y` time ago.
2. randomly walk until you reach a tip.
3. use the tips of the _longest_ two walks as the parents for the new transaction

[2:06]
Is that correct?

Serguei Popov [2:07 AM]

longest -> fastest

[2:07]
also, do you realize that transition probabilities are chosen in a special way?

Micah Zoltu [2:07 AM]
Fastest means shortest since the walkers walk in lockstep?

Serguei Popov [2:08 AM]
means minimal number of steps

Alon Elmaliah [2:10 AM]
the probability of taking a branch (in RW) is proportional to cumulated weight - so longer paths will be chosen more than shorter paths (that have less weight) afaik (edited)

Micah Zoltu [2:10 AM]
> Serguei: Wait, are you thinking that the random walk is _likely_ to choose a shorter path???
> Micah: That is how I understand it from the whitepaper, yes.
> Serguei: The walk will "prefer" a _longer_ path towards the tips.

[2:10]
I must be missing something...

Serguei Popov [2:10 AM]
it seems so (edited)

Micah Zoltu [2:10 AM]
Ah, I see. So it will pick the shortest walk, but when it is stepping it favors longer paths ahead of it?

Serguei Popov [2:11 AM]
yes

Micah Zoltu [2:11 AM]
So the walker pathing algorithm is longest-path-to-tip.

Serguei Popov [2:11 AM]
no

Alon Elmaliah [2:11 AM]
longest-path-to-tip. in NPhard

Micah Zoltu [2:11 AM]
Well, it isn't NPHard if you bake it into the insertion algorithm.

[2:11]
Though, insertion gets very expensive after a while.

[2:12]
Anyway, I'm willing to glaze over the fact that pathfinding longest-path is hard and accept it since I don't think it matters.

[2:12]
If path selection is longest-path, the selfish miner simply generates really long paths to optimize for inclusion by others.

Serguei Popov [2:12 AM]
>So the walker pathing algorithm is longest-path-to-tip.

[2:12]
No, it is not. It is the one described in the paper, with transition probabilities calculated using the cumulative weights.

Micah Zoltu [2:12 AM]
In particular, it targets having a _lot_ of paths that are just the right length to get selected.

Serguei Popov [2:13 AM]
>the selfish miner simply generates really long paths to optimize for inclusion by others

[2:13]
Now look at the "parasite chain" attack to see why it won't work.

Micah Zoltu [2:15 AM]
So transaction weights are historical, they don't know about things built on top of them (unless I'm missing something).

Paul H [2:15 AM]
you're missing something

Micah Zoltu [2:15 AM]
Very possibly.

Paul H [2:15 AM]
they are calculated exactly previous to walking

[2:15]
(currently)

Micah Zoltu [2:16 AM]
Weights are calculated?

Serguei Popov [2:16 AM]
>In particular, it targets having a lot of paths that are just the right length to get selected.

[2:16]
Please, do listen to me. The algorithm is _not_ "select the longest path". I'm just claiming that in "normal" situation it will select a long path (not necessarily the longest one). However, if you try to game it by producing a "long-path-of-yours", you'll fail.

Micah Zoltu [2:17 AM]
Weights, per the whitepaper, are the sum of the weights of the parents.

Paul H [2:17 AM]

> Weights are calculated?
yes

[2:17]
sum of the weights of approving tx

Micah Zoltu [2:17 AM]
So we have a tangle full of transactions that know their _historic_ weight. We don't know how far any transaction is from a tip though (not prior to walkers).

[2:18]
> sum of the weights of approving tx
No?

[2:18]
Sum of weights of _approved_ transactions.

[2:18]
Not sum of the weights of the transactions that approve me.

Paul H [2:19 AM]
no it's not

Serguei Popov [2:19 AM]
cumulative weight = sum of weights of the tx's that approve the given one (directly or indirectly)

Micah Zoltu [2:19 AM]
Page 5 of the whitepaper, Figure 1 has a tangle graph with weights on it.

[2:19]
The arrows point from right to left.

Paul H [2:19 AM]
direction of approval

Micah Zoltu [2:19 AM]
Is Genesis block on the left or the right?

Paul H [2:19 AM]
left

Micah Zoltu [2:20 AM]
So if I submit a transaction, I _approve_ two other transactions by making them my parents. (edited)

[2:20]
When that happens, do I then _update_ both of my parents with new weights?

[2:20]
If so, do they then update _their_ parents with a new weight?

Serguei Popov [2:21 AM]

yes

Micah Zoltu [2:21 AM]
Does every transaction insertion update the _entire_ tangle with new weights?

Serguei Popov [2:21 AM]
yes

Micah Zoltu [2:21 AM]
Surely that doesn't scale...

[2:21]
I'm guessing there is some upper bound after which you stop updating weights?

Paul H [2:21 AM]
simple

[2:21]
you don't do it in that direction

Serguei Popov [2:22 AM]
you don't need to calculate weights to the left of the starting point of the walk

[2:22]
because the walk goes to the right

Micah Zoltu [2:22 AM]
If I'm not maintaining the state of weights of all transactions, then I can't "pick heavy weight" for walk start points.

[2:23]
In order to know the weight of a transaction I need to _first_ walk from left to right.

Paul H [2:23 AM]
sure you can, and there are a lot of ways to do it

[2:23]
which is ideal, I'm not sure (edited)

[2:23]
but I have some ideas

Micah Zoltu [2:23 AM]
One option is to maintain weights of all transactions (perhaps with upper bound) and every time a new transaction arrives update the weights of all transactions it approves (up to upper bound).

Paul H [2:24 AM]
bad option

Alon Elmaliah [2:24 AM]
I think we should decide if the discussion is theory or implementation.
no need to jump in between imo. (edited)

Micah Zoltu [2:24 AM]
Another option is to take your available population and walk up the chain from each of them to calculate the weights.

Paul H [2:24 AM]
the other option is to take a periodic sample starting from some depth

[2:24]
and picking a new heavy-weight point of reference

[2:24]
aka

[2:24]
milestone

[2:24]
hashtag notmath hashtag sorry (edited)

Micah Zoltu [2:25 AM]
OK, so we pick `n` random transactions and walk up the tangle for all of them to get their weights. Then of those we pick `m` of them to use as starting point for the walkers? (edited)

Serguei Popov [2:25 AM]
(serving myself some cognac and calmly observing the discussion :smile:)

Paul H [2:25 AM]
hehe

[2:26]
start from some place decided beforehand (initially genesis)

[2:26]
walk forward to some height

[2:26]
do that n times

[2:26]
pick the one that you arrived at the most times

Micah Zoltu [2:27 AM]
This is still parent selection strategy, right?

Paul H [2:27 AM]
it's a similar algorithm, but no

[2:27]
it's a reference selection strategy

[2:27]
instead of stopping at a tip

[2:27]
you stop at height n

projectShift (Ricardo)
[2:28 AM]
Time to go for me, already 1:30 AM
This channel as become a summer fest :+1:
To be continued ... archiving :slightly_smiling_face:

Paul H [2:28 AM]
alright,
Ricardo's going to bed

[2:28]
better stop this mess

[2:28]
this is also a way to keep a sane main tangle without coordinator

Micah Zoltu [2:28 AM]
I'm trying to understand the parent selection strategy. If I understand what @mthcl has described, in order to select a parent you need to _first_ know the weights of transactions that are part of the population you are selecting from.

Paul H [2:29 AM]
you read code?

[2:29]
spaghetti style (my favorite)?

Micah Zoltu [2:29 AM]
I read code for a living, but try to avoid it as much as possible. :wink:

Paul H [2:30 AM]
well, this is hopefully concise:
https://github.com/iotaledger/iri/blob/master/src/main/java/com/iota/iri/service/TipsManager.java#L277 (edited)

[2:30]
(we use a serial, not recursive method, but the recursive one is easiest for any average coder to comprehend, I hope) (edited)

[2:31]
serial:
https://github.com/iotaledger/iri/blob/master/src/main/java/com/iota/iri/service/TipsManager.java#L230 (edited)

Dhruv Kumar [2:32 AM]
@paulh reminder for you about that blog for explaining such bits in the form of a blogpost because many people are not as well read about the crypto world or the tech behind iota. I think it would be great and would definitely dial down the explanation work that you guys have to do and Ricardo's work as well! :slightly_smiling_face:

Micah Zoltu [2:32 AM]
So that looks like a simple, calculate weight as needed strategy.

Paul H [2:32 AM]
exactly

[2:32]
@dhruv you are very right

Paul H [2:32 AM]
maybe I'll write "Mastering IOTA" someday

2 replies Last reply today at 2:38 AM View thread

Dhruv Kumar [2:33 AM]
haha not someday man, soon-day :stuck_out_tongue:

Micah Zoltu [2:33 AM]
So I go to choose a parent. The weights of transactions aren't stored anywhere, but I can calculate the weight of any one transaction with that function.

Paul H [2:33 AM]
yes

[2:33]
though that function uses own weight as 1

Micah Zoltu [2:34 AM]
From here there are a couple options:
1. Calculate the weights of all transactions in the eligible population.
2. Calculate the weights of a random sampling of transactions in the eligible population.

Paul H [2:34 AM]
walks are done as random(sqrt(weight))

Micah Zoltu [2:34 AM]
It sounds like you are using (2)? (1) could become prohibitively expensive if eligible population is large.

Paul H [2:34 AM]
calculating the weight of all approving transactions

[2:36]
you could just start at a height

[2:37]

and sample from that height to another

[2:37]
no need to traverse any historical stuff below some height

[2:38]
but picking some depth is ideal to find the "best"

Micah Zoltu [2:38 AM]
I'm referring to "eligible population" as the set of transactions that have some persisted state that they can be filtered by.

[2:38]
e.g., "all transactions from 1 hour ago to 30 minutes ago".

Paul H [2:39 AM]
that's a hard thing to pick, I'd probably go by graph topology

Micah Zoltu [2:39 AM]
Presumably in order to choose from a subset of the entire population, they need to be indexed by something.

[2:39]
Alternatively, choose randomly from the population.

Paul H [2:39 AM]
I like to roll the dice

Micah Zoltu [2:40 AM]
I'm okay with any, just want to understand it. :slightly_smiling_face:

Paul H [2:40 AM]
but I'd pick based upon some height parameter (probably) (edited)

Micah Zoltu [2:40 AM]
But need to pick one to focus discussion around.

[2:40]
OK, so the node would index all transactions by height (distance from genesis block)?

Paul H [2:40 AM]
(we're talking about _one_ possible specific implementation, btw)

[2:40]
yes, trunk distance

Micah Zoltu [2:41 AM]
OK, so as a selfish actor, my primary goal is to get my transactions into _that_ population.

Paul H [2:41 AM]
into which population?

Micah Zoltu [2:41 AM]
The eligible population for parent selection.

Alon Elmaliah [2:41 AM]
point of entry (starting the RW)?

Paul H [2:41 AM]
not sure.

[2:42]
are we talking about point of entry or tip selection?

Micah Zoltu [2:42 AM]
We have a bucket of all transactions in the tangle. Parent selection is based on a subset of that set, I'm calling this "eligible population". You indicated that eligible population is based on height.

[2:42]
Talking about how the code decides where to place the walkers for parent selection process.

Alon Elmaliah [2:42 AM]
ok, so we are talking about the same thing.

Micah Zoltu [2:43 AM]
Given the set of all transactions, the transaction creation function needs to pick `n` transactions to place walkers on. It is selecting randomly from an eligible population of transactions. That eligible population is based on height.

Paul H [2:43 AM]
So if you want to get in that place, you want most tx to reference you - otherwise, your weight will be too small

Micah Zoltu [2:43 AM]
So as a selfish actor, I take measures to maximize the number of transactions I have that are of the target height.

Paul H [2:43 AM]
blowball?

Micah Zoltu [2:43 AM]
Just talking about getting myself into the eligible population here, not winning the selection yet.

Paul H [2:43 AM]
how would you predict what that height would be for some other user?

Micah Zoltu [2:43 AM]
Eligible selection is _just_ height. I can easily control for that.

Paul H [2:43 AM]
you'll have a very low weight (unless you have more hashing power than all other selfish actors) (edited)

Micah Zoltu [2:44 AM]

Because they are all following the "honest" algorithm which is well known.

Alon Elmaliah [2:44 AM]
but has parameters, like encryption schemes are well know, the parameters the user inserts are important. (edited)

Micah Zoltu [2:44 AM]
Again, not talking about weight yet. Just talking about eligible population for the moment.

[2:44]
Eligible population does _not_ include weight as part of the criteria.

Paul H [2:44 AM]
how will you know what some other user will choose as their height?

Ali Mousa [2:45 AM]
joined #tanglemath

Paul H [2:45 AM]
I do not think you can determine this

Micah Zoltu [2:45 AM]
The algorithm is public knowledge on GitHub.

Paul H [2:45 AM]
So with this strategy, you're essentially hoping that most users will start at some height

Alon Elmaliah [2:46 AM]
>Eligible population does _not_ include weight as part of the criteria.
you can always choose to start off from txs you trust. like Coo now. (edited)

Micah Zoltu [2:46 AM]
@alon.elmaliah That gets us back to the web of trust network that @come-from-beyond was eluding at but never fully described I believe.

Alon Elmaliah [2:46 AM]
no - only 1/a few you trust. you dont need to trust the whole network. (edited)

Paul H [2:46 AM]
different conversation

Micah Zoltu [2:47 AM]
So as the _first_ selfish actor in the system I know that everyone else is using the reference implementation, which is public knowledge. This implementation has an algorithm to determine eligible population. If I know that algorithm, I can purposefully target it with my transaction generation.

Alon Elmaliah [2:48 AM]
>The algorithm is public knowledge on GitHub.
so is AES (well sort of) -- the depth a user chooses to start walking from is un-known. so is his uniqu POV of the tangle. (edited)

Micah Zoltu [2:48 AM]
@alon.elmaliah How so?

Pranav Gaddamadugu [2:48 AM]
joined #tanglemath

Alon Elmaliah [2:49 AM]
it's a parameter in the API curently -"depth"

Micah Zoltu [2:49 AM]
The client could be setup to start walking from a _random_ height, but that would still need bounds to prevent the client from randomly selecting a height of 1.

[2:49]
Also, you can't build the eligible population from depth as that isn't persisted (no index).

[2:49]
The eligible population must come from data available at the time the transaction was first seen.

[2:49]
Since it is not feasible to update the entire tangle with every new transaction.

Alon Elmaliah [2:50 AM]
i think we lost sync again :slightly_smiling_face: (edited)

Micah Zoltu [2:50 AM]
> We have a bucket of all transactions in the tangle. Parent selection is based on a subset of that set, I'm calling this "eligible population". You indicated that eligible population is based on height.

> Given the set of all transactions, the transaction creation function needs to pick `n` transactions to place walkers on. It is selecting randomly from an eligible population of transactions. That eligible population is based on height.

[2:51]
The reason it can't be based on depth is because the client cannot realistically maintain an index against depth for the full tangle.

Alon Elmaliah [2:51 AM]
>Also, you can't build the eligible population from depth as that isn't persisted (no index).
if we are talking impl. -
currently each tx has a given height.
you can select the starting point based on height - which height is given by the user (using depth param)

Micah Zoltu [2:51 AM]
And if you don't have an index, you can't have an eligible population. If you don't have an eligible population, then your selection must be from _all_ transactions in the tangle which is also infeasible.

[2:52]
So `depth` == `height` in this context?

Alon Elmaliah [2:52 AM]
`height == max_trusted_height-depth` (edited)

Micah Zoltu [2:53 AM]
So this must necessarily be dynamic because the tangle is ever growing. If I start with a `height` of 1 and then the tangle grows to a height of 1,000,000 selecting from a population with height 1 will kill my client.

[2:53]
I'm guessing you mean though, "Height from COO" which is Proof of Authority based and not the solution after July.

Alon Elmaliah [2:55 AM]
you can set any address to give you a sense of height.
you can also give a specific tx to start walking from.

Micah Zoltu [2:55 AM]
OK, so that then depends on having some mechanism for defining what "base" to trust.

[2:56]
Either you have proof of Authority (centralized)
like the COO or you have a web of trust (very hard problem to solve) or you have a selection algorithm.

[2:56]
If you have a selection algorithm, then _that_ selection algorithm is what a selfish participant wants to target.

[2:56]
If you have one of the other two, this entire conversation is vastly different. :smile:

[2:57]
I actually have no problem with PoA personally, but it _isn't_ decentralized (loses buzzword power).

[2:57]
Web of trust: I'm interested in hearing if you think you have solved it, but it has eluded people for decades. (edited)

Alon Elmaliah [3:01 AM]
again, I find it hard to follow the jumps between implementation issues & theory of selfish actors.
if you want to debate impl. - i.e. engineering challenges - like how to efficiently sample a set of txs , I'm happy to.
but, if you want to debate the game theory i'm not your guy :slightly_smiling_face: (edited)

Micah Zoltu [3:02 AM]
The two are, unfortunately, intertwined it seems.

[3:03]
When I ask about the game theory, I get fuzzy answers like, "we'll figure it out". When I ask about implementation, it ends up resulting in what appears to be unsound game theory.

[3:03]
I don't mind focusing on either, but in order to analyze the system a complete solution (either in theory or in practice or in combination) is necessary.

[3:04]
At the moment, it _feels_ like there is hand waving over some of the most complex parts of the system like the web of trust.

Andreas Osowski [10:22 AM]
While I respect that policy, at the moment, this battle is - at the moment - one of who can shout louder until the other one becomes deaf :confused: It's an image issue just as much as a theoretical one right now.

[10:22]
Just see https://www.reddit.com/r/Iota/comments/6hc4o2/concerns_that_must_be_addressed/ which is one of the highest posts on the subreddit atm
reddit
Concerns that MUST be addressed. • r/Iota
Iota seems to have much potential, but the concerns presented by users u/sunnya97 and u/khmoke are not being addressed. *Thanks to these two...

Come-from-Beyond [10:22 AM]
You clearly didn't read the convo

Andreas Osowski [10:23 AM]
I did. I spent the last night following it.

Come-from-Beyond [10:23 AM]
Then what was not convincing?

Andreas Osowski [10:24 AM]
Personally, I think that you and Serguei have proven your points and there hasn't been sufficient opposition.
It's just that for most people the topic is completely above their heads and so the whole issue sadly becomes less a matter of who is right

Tristan [10:25 AM]
So my understanding is that Micah had a misunderstanding of the tip selection algorithm that lead him to believe his attack would be easy to carry out, when really the tangle likely won't confirm his transactions?

Andreas Osowski [10:25 AM]
And I'm not sure whether Micah or Sunny understood the MCMC intuition from a probability theory point of view when setting out on this discussion. (edited)

Come-from-Beyond [10:27 AM]
MCMC is not easy for engineers, you need to be a math guy)

Andreas Osowski [10:27 AM]
I agree.

Come-from-Beyond [10:29 AM]
@tristan Frankly saying, I don't get the idea of the attack

[10:29]
Need more extended description

[10:29]
The text in the pics is pretty vague

[10:29]
working with concrete numbers always helps

Andreas Osowski [10:29 AM]
The idea is just an oversaturation of the available tangle bandwith with the attacker's transactions so that the network is no longer usable and dies. (they called it a 'natural death')

Come-from-Beyond [10:30 AM]
Have you seen how river flows into a sea?

[10:30]
Flow speed is pretty fast on the edge between river and sea

[10:31]
if you go far into the sea from that place you see no signs of the river

[10:31]
water surface is calm

[10:31]
It's similar to what we get when an attacker starts pushing his txs into the tangle via edge nodes

Andreas Osowski [10:32 AM]
They form big deltas.
If you could simulate a tangle with such an attacker in the middle that would split into two subtangles and then reconnect after a while without losing consistency, I'd say you'd have proven a solution to their attack strategy.
But there's no need to discuss this from my point of view right now. I find the amount of nodes that the attacker must be neighboring with infeasible to achieve once iota has grown (edited)

Come-from-Beyond [10:33 AM]
even now it's very hard because we mimick IoT with manual tethering

[10:33]
I can attach you to my node on the edge

[10:33]
generate a lot of txs and push thru my node

[10:33]
and we will watch it

[10:34]
yesterday someone did 300% attack on the mainnet

[10:34]
within 20 mins shockwave was absorbed completely

Andreas Osowski [10:34 AM]
300% of the usual number of txs?

Come-from-Beyond [10:34 AM]
yes, TPS jumped from 1 to 4

[10:34]
http://analytics.iotaledger.net/stresstest.table

[10:35]
last 2 columns show it

Andreas Osowski [10:35 AM]
aye

Come-from-Beyond [10:35 AM]
We did 126 TPS test in the same setup, then it became too expensive to continue, the network wasn't sweating much during 126

[10:36]
So 1000 TPS attack would be handy if we don't pay for it)
