Special thanks to Zack(https://github.com/zack-bitcoin) for participating in this discussion in Zano discord (#general) 14.08.2019

---

zack || Yesterday at 12:43 PM
Hello Zano

Blockchain development is slow today because the process of trial and error is expensive and slow.
Testing out a single idea involves launching a new cryptocurrency, and can cost millions of dollars.

I am trying to develop some mathematical tools which will allow us to calculate whether one kind of blockchain design is more secure than another. https://github.com/zack-bitcoin/amoveo/blob/master/docs/basics/blockchain_engineers_manifesto.md

Once we have math tools like this, it will make it a lot easier to do blockchain engineering, because we can check if a strategy can possibly work without having to actually launch a blockchain.

These math tools are still a work in progress. Please don't take their results too seriously yet.

@crypto_zoidberg invited me here today so that we can look at Zano from the perspective of the math tools I have developed so far.
This might help us to realize if the current design of the math tools has a flaw, and they are incorrectly measuring blockchain security.
This might help us to realize if there is any opportunities to improve Zano and make it more secure.

Here I applied the math tools to Zano, to calculate how secure Zano is:
https://github.com/zack-bitcoin/amoveo/blob/master/docs/other_blockchains/zano.md

Thank you for inviting me here today. I hope that we can discover useful information together. :smiley:

crypto_zoidberg || Yesterday at 4:29 PM
Hello @zack !
Thank you for interest to our project and thank you for your research, it’s much appreciated!
I totally agree with math approach that Zack use to verify security of the particular project, and i’ve done absolutely the same with last Zano whitepaper (additions related in https://github.com/hyle-team/docs/blob/master/zano/PoS_Analysis_and_improvements_proposal.pdf). Basically i have got same mathematical conclusions that Zack got in his document.

The basic assumption that Zack uses is that quite easy to bribe PoS miners, due to “Nothing at stake” problem, which is typical for every PoS system and “Tragedy of the commons“ - every single miner is care about his personal profit, and by setting a bribe for a altchain block makes PoS miners motivated to do mining both alternative chain and main chain.

To make this theoretical attack possible need to have 2 important conditions:
1. Perfect communication channel to majority of PoS miners, to deliver Bribe proposal
2. Coins distribution supposed to be smooth.

Let’s review two this conditions
Zano is privacy coin, so there are no address in the blockchain, it makes additional difficulties for attacker to reach majority of miners, but let’s assume that attacker has some magical channel where he able to reach all PoS miners. The real problem for an attacker is a distribution of the coins. If you take a look in coin distribution of any blockchain project(as far as possible) you’ll find out that there is always majority of the coins focused in a very few groups of major holders. This true for small project’s like we, as well as it’s true for Bitcoin. Hard to explain in detail why this happening, but it’s just a natural thing that happens in every finance environment: https://en.wikipedia.org/wiki/Distribution_of_wealth
Since it’s not much profitable do to PoS mining with relatively small amount of coins at least due to electricity consumptions, the majority of PoS power consist of big holders. Now, with big holders problem of “nothing at stake” became less meaningful, because they have something to lose.

If they help to perform 51% this means that cost of their actives will dropped after. So the bribe now should become something relatively close to amount of coins to lose, which now makes this attack way more expensive.
Now, let's go back to pure PoW miners. the problem of pure PoW systems is mining pools, which leads to "de-decentralisation". Is you take a look into current Bitcoin mining hashrate distribution: https://btc.com/stats/pool you'll see that 51% of hashrate belongs to 3 mining pools. And this situation is nearly the same for most of the PoW blockchains. And if we talk about average pool owner - then same bribe is possible but it's going to be cheaper - you need to cover expense of mining of 10/20 blocks, may be something on top of it, but this is way less then bribe to majority coin holder.

So, i can conclude that from practical point of view hybrid PoW/PoS is the best choice in a current technological level.
But i also agree that invention of consensus which will resist against mentioned problems is highly desirable and we'll keep working hard on that.

zack || Yesterday at 4:58 PM
"Zano is privacy coin, so there are no address in the blockchain, it makes additional difficulties for attacker to reach majority of miners"

If the zano block creators can get paid a bribe by breaking privacy, then it will be in their interest to break privacy. I am not aware of any cryptosystem that prevents them from breaking privacy if they want to do that. Keep in mind that they can spend their money, and then reveal their private key, and that they can take timestamped signed messages at any time.

"there is always majority of the coins focused in a very few groups of major holders"

The level of centralization of hashpower and of staking power are very different things. Miners cooperating in a mining pool is game theoretically very different from a single individual owning a large portion of the stake in a PoS blockchain.
If a mining pool operator does something strange, all the miners will abandon their pool.

If someone takes majority control of a PoS blockchain, they can permanently alter the rules in arbitrary ways. They can set it up so it is impossible for them to ever lose power.

If someone has a mining pool with >50%, they could censor txs for a few days, until the miners find out what is happening and switch pools. And then the miners leave and their pool is worthless.

If there are 5 people who own each own 10.2% of the voting power of a decision.
And the decision could result in each of them losing $100, if B should win, or they keep their money if A should win.
This is similar to the situation you are describing, with a high level of centralization.
According to tragedy of the commons, I would only have to bribe each one about $10 to convince them to vote for B.
So for $50, I could destroy $1000 of stake, and probably a lot more value on the blockchain itself.

If these 5 people can cooperate to ignore my bribe, then they can cooperate to change the rules to extract higher rents from the users.

The level of security of a system is inversely related to the cost of using that system.
If there is someone who can break your blockchain, you will need to pay them bribes to convince them not to break it. If it is cheaper or more profitable to break, then the bribes will need to be higher.

If it is very easy for these 5 people to make arbitrary changes to the rules to extract more rents, then we will need to be paying them enough fees to convince them not to do that.

The comparison to PoW is not accurate. In PoW it is impossible to punish censorship, so if someone tried bribing a coalition to make changes, it is impossible to punish any sub-coalition from doing a soft fork to make arbitrary changes to the rules, taking the bribe, and causing the attack to fail.

This makes it so that no one is willing to join a coalition. Since they know it is just a trick to steal their hashpower.
So it is not possible to bribe miners to form coalitions to take control of PoW consensus.

In PoS systems everyone has money locked in the system connected to the decisions that are being made. So a coalition can punish censorship in it's members. So the attackers don't have to worry about a soft-fork sub-attack. This makes it so stakers feel confident participating in a coalition. They know it is never in the interest of the other members of the coalition to double-cross them.
Because of this it is cheap to pay bribes and take over PoS systems.

Gigabyted || Yesterday at 5:19 PM
Excuse my ignorance here, but this would work for EVERY implementation of PoS, independantly of the PoS implementation right? Those are general arguments against PoS as a whole, nothing specificaly related to Zano PoS implementation, am i wrong?

haha || Yesterday at 5:19 PM
Those arguments still apply to zano pos though

Gigabyted || Yesterday at 5:21 PM
Is there any known case of such an attack over a PoS blockchain so far that you are aware of?

zScrypte || Yesterday at 5:21 PM
As per my understanding here, 5 users with each 10,2% of the PoS voting power would be a 51% on the PoS chain if they where to form a "coalition". but still at this point they would also need a huge portion of the PoW chain in order to alter the consensus rules...

zack || Yesterday at 5:22 PM
With pure PoW, you need 51% hashpower.
With pow/pos hybrid you can cheaply disarm the PoS half of the system, and then you need something <50% of hashpower to take control.

Gigabyted || Yesterday at 5:22 PM
In a PoW/PoS hybrid consensus, lets say someone owns 60% of the PoS, how does this affect PoW, does he need lower than 51% to attack the pow consensus?

zack || Yesterday at 5:22 PM
I wrote a PoS/PoW hybrid doc that was linked to from the zano review doc
to really prove it
once the PoS part is disarmed, you need <50% hashpower to take down the PoW part.

Shea (UTC+1) || Yesterday at 5:23 PM
@Gigabyted yeah i think Zack had some calculation with exactly 60% pos power assumed. Its needed around 45% pow if i remember

Gigabyted || Yesterday at 5:23 PM
Is it possible to run (or build) a table that would take into account zano distribution and pos implementation and see with different PoS ration owned how it would affect zano PoW?

zack || Yesterday at 5:24 PM
yeah, you can see that in the zano whitepaper. it is really a great document

Gigabyted || Yesterday at 5:24 PM
Owning 60% of PoS only reduce the pow requirement by 5% ?

zack || Yesterday at 5:24 PM
No

if you have 90% PoS, then the PoW requirement goes down to 5%.

zScrypte || Yesterday at 5:24 PM
Owning 90% of t he PoS takes it to 5,2% @Gigabyted

Gigabyted || Yesterday at 5:25 PM
any way to draw a curve of this for zano?
and also do estimate over how hard it gets to own that % of PoS over zano distribution?

Shea (UTC+1) || Yesterday at 5:25 PM
Is that number for Zano specific? Cause i remember some numbers from Zack document about pow/pos

Gigabyted || Yesterday at 5:25 PM
well zano is a privacy coin, so getting the distribution alone is hard
Also lets pretend a sucess full 51% attack is done over it, the most common case is a double spend right?

zack || Yesterday at 5:26 PM
in my pow/pos document, I make a general proof that it is not possible to define a fork choice rule such that pow/pos hybrid costs >50% hashpower to attack, if you have already disarmed PoS.

Gigabyted || Yesterday at 5:27 PM
What kind of effect a 51% attack has over a chain? beside the exchange that lose funds does it have other impact over a chain?

zack || Yesterday at 5:27 PM
Security is important even if no attack occurs. Because the cost to use a system is inversely related to how secure it is.
The more secure systems can charge lower fees and undercut the cost of the less secure system. the more secure systems out-compete the less secure ones.

Gigabyted || Yesterday at 5:27 PM
(sorry im asking too many questions)

zack || Yesterday at 5:28 PM
the attack I am describing, it doesn't matter if we know the distribution of stakeholders.

Gigabyted || Yesterday at 5:28 PM
also is the opposite true, if someone have 90% of the pow, does he need to bribe less holders to own it?

zack || Yesterday at 5:28 PM
I think so. if you have majority PoW, then you would need <50% of the PoS in order to take control.

Gigabyted || Yesterday at 5:29 PM
aint it cheaper to own 90% of the PoW than 90% of the pos over zano right now?

zScrypte || Yesterday at 5:29 PM
Gigabyted
:
well zano is a privacy coin, so getting the distribution alone is hard

But lets say we have 7 members that are major holder, about 60+ % of the coins, most likely know each others.

then they could create a coalition by themselves in order to modify consensus rules with little support from others.

zack || Yesterday at 5:29 PM
Usually when you combine security tools, the result is less secure.
Because we end up in a case where the attacker has more choice for which direction they can attack from.
The system is as weak as the weakest link.
owning 90% PoS is very expensive. but bribing the holders of 90% of the stake can be cheap.

Gigabyted || Yesterday at 5:30 PM
i guess if zano pow was MUCH larger, owning PoS could be cheaper if alot of power is spent over securing the chain (thru pow)
so i guess that when pow reach a certain mass, it could get cheaper to bribe holders to reduce the cost of a pow attack

zack || Yesterday at 5:31 PM
@zScrypte well 60% of the coins does give them a big advantage. They would still either need like 40% of the hashpower, or to bribe a lot more of the coin holders.

Gigabyted || Yesterday at 5:31 PM
but im curious to see where this would be

crypto_zoidberg || Yesterday at 5:33 PM
wait, guys, let's slow down please

Gigabyted || Yesterday at 5:33 PM
right now zano PoW is about 6ghs and a single RX 580 can do about 10mhs and i can rent this for about 50c right now
sorry, i will let you guys speak and clear out the assumptions that were made
right now i could double the zano hashrate for about 300$ (for a day)

crypto_zoidberg || Yesterday at 5:35 PM
@zack first of all little clarification:
"if you have 90% PoS, then the PoW requirement goes down to 5%." - that is not correct for Zano, please check formula and graph. Even if you have 90% PoS you need at least 20% of PoW

"If a mining pool operator does something strange, all the miners will abandon their pool." - absolutely disagree. It all the same, and even worse - in mining business hashpower now is just selling on open market, and rig owners absolutely unaware of how it got used.

zack || Yesterday at 5:37 PM
900 000 on the vertical axis seems to line up with around 1500 on the horizontal axis. Which would indicate 90% - 8.3%
Maybe I am not reading this correctly.

crypto_zoidberg || Yesterday at 5:38 PM
the point in the graphs shows 50% for both graphs
4000 on PoW axis is 50% of PoW
40000 on PoS axis is 50% of PoS

zScrypte || Yesterday at 5:39 PM
8000 being 100%?

crypto_zoidberg || Yesterday at 5:39 PM
yep

zScrypte || Yesterday at 5:40 PM
okay yeah, just noticed the straight line

crypto_zoidberg || Yesterday at 5:41 PM
also to consider about this graph - 80000 of PoS is a 100% of current hashpower, but it's not 100% of all coins, because typically not all coins involved in mining

zack || Yesterday at 5:41 PM
This is my understanding of Zano's fork choice rule
weight(P, H) = (P + H) * (P * H)^2

where P is the portion of stake participating in that version of the fork, and H is the portion of hashpower.

crypto_zoidberg || Yesterday at 5:42 PM
it's not precise
https://prnt.sc/osnmvt
Lightshot
Screenshot

here is precise formula of fork chosing
and graph built by this formula in math emulator

zack || Yesterday at 5:42 PM
I think it is the same, I am just simplifying.

crypto_zoidberg || Yesterday at 5:43 PM
https://www.desmos.com/calculator/nhzf7mbtes

zack || Yesterday at 5:43 PM
it doesn't make sense to graph more than 100% of the stake

crypto_zoidberg || Yesterday at 5:43 PM
"I think it is the same, I am just simplifying." i think simplification is not correct
"also to consider about this graph - 80000 of PoS is a 100% of current hashpower, but it's not 100% of all coins, because typically not all coins involved in mining" - here is explanation
PoS hashpower and total coins is different
coins are normally more

zack || Yesterday at 5:46 PM
Your fork choice algorithm is complicated because you can only know relative weights.
But I think I can prove that any self-consistent system of relative weights is equivalent to some system of absolute weights.

As long as your system of relative weights has the rule that
A>B and B>C implies A>C

crypto_zoidberg || Yesterday at 5:48 PM

well, i can prove that my fork choice algo follow this graph, exactly because it's built on this formula, and numbers are have to fit this graph, so statement about 90PoS + 5% PoW is wrong. This formula proves it. this graph illustrate it.
the goal of this formula was to achieve this behaviour

zack || Yesterday at 5:50 PM
yeah, I probably made a mistake while simplifying, but I still think a system of absolute weights is not only easier to explain, but it would also let you write better software.
because you don't have to re-calculate relative weights every time there is a small fork

crypto_zoidberg || Yesterday at 5:53 PM
the code is already done, and it's O(1) because we have all data kept for every block, so it's cheap calculation, nearly the same as it was in original algo.

zack || Yesterday at 5:53 PM
O(1) with respect to what?

crypto_zoidberg || Yesterday at 5:53 PM
anyway, let me read the rest of your post :wink: i still didn't answer to other points
O(1) with respect to len of the subchain

zack || Yesterday at 5:54 PM
oh, I was thinking about it in terms of the number of times a fork happens.
like, what if there are 2 sides, and they keep trading off being longer.
so for 50 blocks in a row, it switches from one to the other
if every block has an absolute weight, then we never have to calculate the weight of any individual block more than once. O(50)
but with your current algorithm, it seems like this would be O(50^2 / 2) times a block's weight is measured

Gigabyted || Yesterday at 5:58 PM
(just want to clarify, @zack dont be fooled by my poor choices of words (my english aint always good) but its not my intent to attack you at all, i believe we are bless to have you in here and its a epic moment to witness! Sorry if anyone believed that i was trying to defend zano or attack your arguments here)

crypto_zoidberg || Yesterday at 6:01 PM
"but with your current algorithm, it seems like this would be O(50^2 / 2) times a block's weight is measured" - nope, it's just use cumulative difficulties which is precalculated for every block once. actually i take cumulutive difficulty at point of split substract if from it from current blocks' cumulative difficulties and then perform arithmetics.

zack || Yesterday at 6:03 PM
ok, it sounds like the cumulative difficulties are a way to collapse the information the same way
so the cumulative PoW difficulty is in unites of hashes computed, and the cumulative PoS difficulty is in coin*hours staked?
I was confused before. I thought these difficulties were for changing the price of participating as PoW or PoS.
to maintain the rate of block production

Alfred || Yesterday at 6:09 PM
I'd like to ask a question about that common assumption I see when referring to PoS and 51% attacks:
If they help to perform 51% this means that cost of their actives will dropped after.

I don't see any direct correlation between price and a 51% attack happening. To me it comes down to say that if a robber would rob a bank (thus demonstrating some insecurities in the system) the price of USD would crash as a result.
Do you guys have any clarification on that topic or am I just missing something obvious?

zack || Yesterday at 6:11 PM
that's asking the wrong question.
The fact is, whether the price drops or not does not matter.
Voters are still willing to take a cheap bribe and let the system break.

zScrypte || Yesterday at 6:11 PM
Is more like robbing the system in a whole than robbing a single bank

haha || Yesterday at 6:12 PM
@Alfred It's irrelevant to the actual argument but it will definitely drop. You're not robbing a bank, your robbing every single bank

Alfred || Yesterday at 6:12 PM
It's one of the first zoidberg's argument hence my question

zack || Yesterday at 6:14 PM
a soft fork can do any arbitrary changes.
I have used soft forks to update Amoveo before. They are nice because only the consensus level nodes have to update. Exchanges for example don't have to update.
Whether an update is good, or an attack is a matter of perspective

crypto_zoidberg || Yesterday at 6:15 PM
points from original post:
“If someone has a mining pool with >50%, they could censor txs for a few days, until the miners find out what is happening and switch pools. And then the miners leave and their pool is worthless.”
- also disagree - as i said before hashpower is just rented, it’s running as a business and same “Tragedy of the commons”, motivation is just profit.

“If there is someone who can break your blockchain, you will need to pay them bribes to convince them not to break it. If it is cheaper or more profitable to break, then the bribes will need to be higher.”
- unlike PoW miners, PoS miners are holders of coins and they natively motivated to keep blockchain healthy, because of the nature of the PoS. In PoW hashpower miners absolutely neutral to project, they just rent their rigs, mostly management of the hashpower is done by arbitration robots, pure mater of profit. With PoS you stick to the project.

“The comparison to PoW is not accurate. In PoW it is impossible to punish censorship, so if someone tried bribing a coalition to make changes, it is impossible to punish any sub-coalition from doing a soft fork to make arbitrary changes to the rules, taking the bribe, and causing the attack to fail.
This makes it so that no one is willing to join a coalition. Since they know it is just a trick to steal their hashpower.
So it is not possible to bribe miners to form coalitions to take control of PoW consensus.”
- problem of PoW that you even don’t need coalition there, you already have pools there, which control, and normally it’s just a few pools. (Now it’s multipoolsm so the don’t care much about particular blockchain project and not depend of it from business prospective). Also multipools have tend to attack small projects by swelling their difficulty functions so it’s proven that pool’s operators foloow only profit interests.

@Alfred "Do you guys have any clarification on that topic or am I just missing something obvious?" i think comparison with the banks is not correct because in our times every "bank" is issuing it's own currency, and value depends from how strong the protection. Illustration of this is price reaction of blockchain project being hacked of attacked.

zack || Yesterday at 6:18 PM
yeah, I was wrong about miners ditching a bad mining pool. I am glad I was able to learn this from you.

unlike PoW miners, PoS miners are holders of coins and they natively motivated to keep blockchain healthy

And PoW miners are holders of ASICS that only work on one blockchain. But as you already explained, this is tragedy of the commons. The value of the mining hardware or the coins doesn't matter. They are still willing to take the bribe and break their blockchain.

crypto_zoidberg || Yesterday at 6:20 PM
agree about ASICS, the only difference is that ASICs is a short term relation lol :smiley: they are getting useless after less then one year holding coins also could be a short term tho
regarding PoW - boolberry was attacked by multipools, i've learned nature of this pity-less business on my own experience

haha || Yesterday at 6:23 PM
"PoS miners are holders of coins and they natively motivated to keep blockchain healthy"
Doesn't the invidual think differently from the masses? If I was offered some money to join an attack, I would gain more money or have the same if the attack succeeded and if the attack didn't succeed by joining in than not joining

Alfred || Yesterday at 6:23 PM
Multiple blockchains have been attacked (XVG multiple 51% - XMR multiple vulnerabilities) and there is no obvious correlation between that happening and the price decreasing other than a natural price downtrend

crypto_zoidberg || Yesterday at 6:25 PM
"Doesn't the invidual think differently from the masses? If I was offered some money to join an attack, I would gain more money or have the same if the attack succeeded and if the attack didn't succeed by joining in than not joining"
- i'm only saying that this rule works both for PoW and for PoS miners. Basically it's not invented yet technology which prevents from double spend attack

haha || Yesterday at 6:26 PM
It doesn't work for PoW as there's no way to form a coalition and ensure that everyone will follow through on the attack
they could just take the money and then keep mining the right chain for example

zack || Yesterday at 6:26 PM
If I am running a mining pool at a loss to try and control the network, and I try to do something that could harm the network by censoring txs. The people I am harming would be willing to pay higher fees to get their txs included.
If the sum of these fees is bigger than how much of a loss I am willing to take by running my mining pool, then someone else would be able to profitably run a competing mining pool and pay the miners even better prices, by including all the txs.

This isn't the case in PoS, because the majority could just endlessly censor any competition and never lose control.
so I think this is only a level 2 attack in PoW. PoW is still level 2 secure.

haha || Yesterday at 6:28 PM
On PoS, can't someone set up a decentralized way to ensure that stakers will join in on the attack?
without smart contracts
@zack
If I bribe someone, for example, I need to 100% know they will join in on the attack and not just keep staking normally after getting the money

jriggs28 || Yesterday at 6:30 PM
So this weakness is heavily reliant on being able to bribe everyone?

zack || Yesterday at 6:30 PM
but is is right up against the edge of being a level 3 attack.

jriggs28 || Yesterday at 6:30 PM
If I owned a large portion of a project why on earth would i put that investment at risk for a bribe that will not cover my losses after the coin in wrecked?

crypto_zoidberg || Yesterday at 6:31 PM
"It doesn't work for PoW as there's no way to form a coalition and ensure that everyone will follow through on the attack
they could just take the money and then keep mining the right chain for example"
- it just a matter business organisation, not a bit problem, and as i said - no need to looking for coalition, pool itself a coalition controlled by one person.

Aiwe Freeman || Yesterday at 6:32 PM
Hello guys, may I throw in my 5 cents? I would like to hear your oppinion on this idea:

The security of PoW is based on the assumption that it is unfeasible to achieve the prevail in a hash rate for a single entity and even if such entity will possess that hashrate it will be economically motivated not to attack network due to its investments in mining infrastructure, which is no longer true.

Zawy stated that “the only thing protecting PoW is the stake of the equipment infrastructure… All the small coins switching to PoW algorithms that can’t be easily rented is an attempt to make miners hold an equipment stake.”

Here's naive and simple solution: add to PoW, what has become missing — a stake. However not in equipment but in coin itself.

So the idea is: in order to mine a block miner must stake the number of coins that is not less than the current minimum amount which is determined by the current difficulty.
A miner forms the coinbase transaction as follows: he sends to himself the amount not less than the required minimum stake and adds fees and block reward. This is enough to prove and verify his collateral stake in a simple way.

There is so called mined money unlock window n, a rule which locks all outputs in coinbase transaction for n blocks. This means that coins from coinbase transaction can be spent only after n blocks. Therefore, to be able to mine blocks successively, miner will have to possess much more money than minimum stake amount for one block, — he will need a stake for each block until his stake for a first mined block is unlocked.

haha || Yesterday at 6:35 PM
@crypto_zoidberg a coallition by a pool is really unstable compared to one with pos holders
No doubt big miners are up to date on their pool's activities

crypto_zoidberg || Yesterday at 6:38 PM
@Aiwe Freeman was thinking about it recently and i guess this will evolve into mining pools which just also have to hold some coins to get right to win the blocks
i think it even make more centralized - miner motivated to join the pool with more coins at stake

haha || Yesterday at 6:39 PM
True what you said about business organisation

Aiwe Freeman || Yesterday at 6:39 PM
I came to same conclusion, however unlike small cost of running pool, pool with stakes will make its operator very loyal to the coin.

haha || Yesterday at 6:40 PM
Is it illegal to 51% attack a blockchain?]

crypto_zoidberg || Yesterday at 6:40 PM
@Aiwe Freeman agree, but to mach centralisation. so need something else to oppose PoW

Alfred || Yesterday at 6:40 PM
double spending is a robbery imho @haha

crypto_zoidberg || Yesterday at 6:41 PM
@haha i think it is legal, since this is even coded in core to handle this altchains stuff :smiley:

Alfred || Yesterday at 6:42 PM
yea it's by design - but when an exchange gets stolen $200k as a result of an intentional double spend then I think it's a robbery

crypto_zoidberg || Yesterday at 6:43 PM
looks like robbery is legal in crypto :smiley:

haha || Yesterday at 6:43 PM
I guess that's an argument against both PoS and PoW
if it is a robbery

crypto_zoidberg || Yesterday at 6:43 PM
actually i think ICO is even worse robbery

Aiwe Freeman || Yesterday at 6:44 PM
What about just reject alt. chain if some transaction in it is missing?

crypto_zoidberg || Yesterday at 6:45 PM
was also thinking a lot about this
but the problem is
in that case is supper easy to split the network

Aiwe Freeman || Yesterday at 6:46 PM
only newly joining nodes can be lured into split, others will follow public majority

zack || Yesterday at 6:46 PM
How about I use an ICO to fund a soft fork attack to take control of a PoS blockchain. and once I have control, I print new money and give it to ICO participants, and then finally upgrade from PoS to something secure.
Is that ICO still robbery?

crypto_zoidberg || Yesterday at 6:47 PM
i can perform two altchains one with transaction A in no transaction B, and other subchain with B in it and no A in it, and then i'll push to part of the hosts fist subchain and second part - another subchain, and network is splitted, all the mess around :smiley:

Aiwe Freeman || Yesterday at 6:48 PM
99.99% of ICO is a robbery

crypto_zoidberg || Yesterday at 6:48 PM
@zack now ICO is supper robber :smiley: because you actually put this storry in whitepaper, but we all how ICO running - you can perform an attack but don't have motivation to return money to ICO holders :smiley:
at least i was tend to think ICO works this way lol

zack || Yesterday at 6:49 PM
haha, that would be pretty hilarious.
Double-crossing the band of thieves, and walking away with everything.

crypto_zoidberg || Yesterday at 6:50 PM
i'm pretty sure there will be people who will keep invest into this ICO even after you perform the job and dissapear :smiley:
so you can run second round :smiley:

Aiwe Freeman || Yesterday at 6:54 PM
@crypto_zoidberg unless txs in subchains are mutually excluding (spend same coins to different destinations) they will unite after some part will mine other's part tx

crypto_zoidberg || Yesterday at 6:55 PM
if this TXs contradict each other ?

Aiwe Freeman || Yesterday at 6:55 PM
yes, they have to contradict

crypto_zoidberg || Yesterday at 6:56 PM
fo example spend same out
then it's collision
game over :smiley:

Aiwe Freeman || Yesterday at 6:56 PM
yes, if they don't contradict each part will just have missing txs in mempool and mine them into a block then they will unite by usual nakamoto rule
so only clear double spend can split the net

crypto_zoidberg || Yesterday at 6:57 PM
if we can build system which wold verify against absent transaction in altchain then we can assume double spend attack as fixed.
not only double spend, just two transactions which can't be measured, then network is f#$ked.

Aiwe Freeman || Yesterday at 7:00 PM
yes, also spending reward coins from newly mined block from alt chain if unlock window is small will cause the split

crypto_zoidberg || Yesterday at 7:00 PM
why?
we handle this sittuation
i believe we do :smiley:

Aiwe Freeman || Yesterday at 7:01 PM
they don't exist in other chain, so tx will be illegal in other chain and thus it will be rejected
maybe i'm wrong :smiley:

crypto_zoidberg || Yesterday at 7:03 PM
i mean this tx can be there, in alchain it exists properly, but any node can perfectly reoranize to other subchain without problems, same with main net - if althcain got more cumulative difficulty there - main will be swaitched with bo problems.
but if we have some rules for comparing tx set for subchain - then it can be only one way ticket, and then net can be splited
i've been thinkin about this problem for a long time, but was unable to find proper stable solution, i thin a lot of devs thinking about it

zack || Yesterday at 7:05 PM
Even though Zano is weaker than PoW in some technical sense, it seems like it is a better solution for now.

Because if someone started doing these PoW/PoS hybrid bribery attacks, there are a lot of other blockchains that are easier to attack than Zano, so you will have plenty of warning to switch to PoW at that point in time.

And until then the PoS aspects of Zano are giving good protection from hashrate rental attacks.

Aiwe Freeman || Yesterday at 7:07 PM
perhaps avalanche gossip protocol can be used in case of split to form the consensus however i doubt this is perfect solution

crypto_zoidberg || Yesterday at 7:08 PM
@zack With all respect i absolutely disagree with that. Zano need way more resources to perform double spend attack - you need to bribe majority of PoS holders (which is nearly impossible for Zano and for many projects due to distribution) AND you need to have hashrate power to take over.
Pure PoW is way more easier to attack as form technical perspective as from organisational perspective

Alfred || Yesterday at 7:10 PM
I think the organisational perspective is interesting to take into account - but it's a hard thing to quantify
but that should definitely be factored into attack cost

zScrypte || Yesterday at 7:17 PM
Using zack formula we can see the the graph is not the same a zano formula... There must be something wrong in the simplification no?

crypto_zoidberg || Yesterday at 7:17 PM
i think zack already said that his simplification was wrong

zack || Yesterday at 7:18 PM
The reason I think Zano wont be attacked first is not because the validators are hidden by encryption, or because they are more centralized.
It is because you have such a great fork choice rule. A lot better than other projects I have looked at.
as I explained before. hiding validators behind encryption doesn't prevent bribery.
And unless there are 3 people owning >50% of stake, you can't prevent bribery by maintaining centralized control.
the validators break encryption on purpose to win more bribes.

crypto_zoidberg || Yesterday at 7:20 PM
"as I explained before. hiding validators behind encryption doesn't prevent bribery." - and i agreed with this.

zack || Yesterday at 7:21 PM
an attacker can bribe the half of validators who own less stake.
Even if 40% of stake is owned by 2 rich people, we can focus on bribing the other 60%.

crypto_zoidberg || Yesterday at 7:21 PM
thanks for kind words regarding fork choice
and thank you for this debates, it's much appreciated !
you always welcome to our chat with your research and critics!

zack || Yesterday at 7:25 PM
I wonder about more applications of fork choice rules like this.
If I set up a consensus that was 99% proof of work, and 1% developer's choice.

So if there is a fork, whichever side the devs prefer will have a 1% advantage in weight.

zScrypte || Yesterday at 7:26 PM
i think that can become a trust issue in the long run

zack || Yesterday at 7:27 PM
if the dev reveals their private key, the both sides of the fork have the 1% advantage forever and it cancels out

crypto_zoidberg || Yesterday at 7:28 PM
giving to devs any power above other participants will destroy all equilibrium i guess. At least this is what i was learned from what i've seen in other projects

zack || Yesterday at 7:28 PM
if my blockchain is 1% more expensive to attack, then I can theoretically charge 1% lower fees, and that is enough to out-compete the competition.

crypto_zoidberg || Yesterday at 7:30 PM
having 1% make same cost for 51% attack i believe
or i didn't get how it prevents

zack || Yesterday at 7:31 PM
if one side has 50.4% hashpower, and the other has 49.6% I could give my support to the weaker side, and bump it up to 50.6%
it probably isn't a useful mechanism.

zack || Yesterday at 7:42 PM
Thinking about the fork choice rule.
I think I see a symmetry rule we can use to understand these formula better:

If having P% of normal levels of stake and H% of normal levels of Hashpower is > weight than consensus.
Then that means having H% of normal levels of stake and P% of normal levels of Hashpower is < weight than consensus.
no nevermind. sorry. ill think about it more and come back if I have anything.

crypto_zoidberg || Yesterday at 7:46 PM
not really sure how this 1% supposed to work, but it's something which use human factor i guess, so devs should be aware of attack of something? anyway, so attacker need to buy hashrate to get 51% of hashrate compared to "fair" miners. if we talk about buying hashrate (bribing pool owners is different right?)
then i think it's not matter that there is some 1% of super fair miners(devs).

zack || Yesterday at 7:46 PM
do you know any symmetries for the fork choice rule?
your graphs all seem symmetric over x=y

crypto_zoidberg || Yesterday at 7:47 PM
it should be symmetric
well, i wanted them to be symmetric

zack || Yesterday at 7:48 PM
so we established that if I have 90% stake, I would need 20% hashpower to take control.
Does that then mean that if I had 90% hashpower, I would need 20% stake to take control?

Gigabyted || Yesterday at 7:49 PM
(thanks for taking back my question @zack!)

crypto_zoidberg || Yesterday at 7:49 PM
@zack yep

Mr J say || Yesterday at 7:49 PM
@Gigabyted saw your tweet! Very good read this discussion

zack || Yesterday at 7:50 PM
good to know. thanks @crypto_zoidberg

crypto_zoidberg || Yesterday at 7:52 PM
i was intending to make fork choice rule that make altchain with majority of one type of power (PoS or PoW) harder to create/harder to take over. That's why it looks like that.
but you can do that only by comparing two subchains, so that's why formulas are system of two equations.

zack || Yesterday at 8:00 PM
What about long-range attacks in Zano?
If I buy up a bunch of private keys from some point in history, and then rebuild from there.
If I can rebuild with a much higher portion of validator participation, then I don't need much hashpower to rewrite history.
if average participation is 20%, I could buy up 40% from some point in history, and then I would need very little hashrate to rewrite everything.

crypto_zoidberg || Yesterday at 8:08 PM
checkpoints won't let you do that - first, second you still need a lot of PoW to perform the attack - because PoW for long distance - it's going to be very expensive.

zack || Yesterday at 8:09 PM
what if I attack at a block between now and the most recent checkpoint?
then there isn't so much history to re-write
bribing validators to give me an old copy of their private key is a lot easier in comparison to convincing them to stick an active private key into an alternative version of the software that I wrote.
usually long-range attacks are solved by a combination of checkpointing and security deposits.
But since your validators use encryption to hide their identities, I think you cant confiscate deposits to enforce this.

crypto_zoidberg || Yesterday at 8:15 PM
good point, but even with majority of PoS old keys you need 20% of hashrate, and for long range attack it's way more more more then 50% PoW for low range attack(last 10-20 blocks), right ?
for PoW in long range it became math integral

zack || Yesterday at 8:20 PM
if you have 20% more hashpower than the rest of the network, and you are trying to rewrite history, you will need to mine for 5 hours to catch up 1 hour of history.
but if you have 100% more hashpower, you only need to mine for 1 hour to catch up by 1 hour.

BuzzkillB || Yesterday at 8:27 PM
how much PoS out of the circulating do you need to do that POW attack?

zack || Yesterday at 8:28 PM

if you want to make the PoW attack less expensive vs attacking a pure PoW blockchain, then you need to control at least 50% of the active validator stake.

Aiwe Freeman || Yesterday at 8:29 PM
I saw very simple solution, just limit reorg depth to say 10 blocks and you solve long range reorg and 51%-attack problem. Well, this comes at cost of permanent split possibility.

zack || Yesterday at 8:30 PM
so what if I launch a long-range-attack at a depth of 5 blocks?

Aiwe Freeman || Yesterday at 8:31 PM
If it's 5 blocks from the chain tip it's not long-range (how many blocks do we need to qualify for long-range?) and reorg can happen.

zack || Yesterday at 8:32 PM
"long-range-attack" means you buy up old private keys that no longer have value. keys that had previously controlled validator stake.
maybe I shouldn't call it that. the name is confusing.

crypto_zoidberg || Yesterday at 8:32 PM
"I saw very simple solution, just limit reorg depth to say 10 blocks and you solve long range reorg and 51%-attack problem. Well, this comes at cost of permanent split possibility."- unfortunately it's not working this way, as soon as you limit reorganize len then i can split the net.

BuzzkillB || Yesterday at 8:32 PM
how much of those keys do you need??

Aiwe Freeman || Yesterday at 8:33 PM
I know, but nodes will reject your alt. chain if split is deeper than 10 blocks from their tip.
@crypto_zoidberg that's why i stated that this comes at cost of split possibility.

zack || Yesterday at 8:33 PM
@crypto_zoidberg How do I take advantage of the 10 block checkpoint to cause a split effectively?

crypto_zoidberg || Yesterday at 8:34 PM
"f you have 20% more hashpower than the rest of the network, and you are trying to rewrite history, you will need to mine for 5 hours to catch up 1 hour of history.
but if you have 100% more hashpower, you only need to mine for 1 hour to catch up by 1 hour."

- it's all the same from cost perspective. Cost is a hashrate * time.

Aiwe Freeman || Yesterday at 8:34 PM
Yes this is like kind of 10 blocks trailing checkpoint :smiley:
athough this type of checkpoint is individual to each node

zack || Yesterday at 8:35 PM
it's all the same from cost perspective. Cost is a hashrate * time.

No.
If I have 1.2x as much hashpower as the network for 5 hours, that is 1.2*5 = 6 units of hashpower.
if I have 2x as much hashpower as the network for 1 hour, that is 2 * 1 = 2 units of hashpower.

But in each case, I have caught up by 1 hour of history.
the rest of the network is still growing during the attack. so if you take longer, they have more time to build defense.
a faster attack is cheaper
assuming that hashrate is liquid enough

crypto_zoidberg || Yesterday at 8:41 PM
it's a bit things that you talking, you talk more about races i guess. But, when we estimate two different subchines we check cumulative difficulty, which reflects actual hashing opreations that was performed. (with some quantization error). So basically it's all reflect number of hashing operations.

zack || Yesterday at 8:42 PM
if I do 1.2 gigahashes per second for 5 hours, I will have computed 3x more hashes in comparison to doing 2 gigahashes per second for 1 hour.

crypto_zoidberg || Yesterday at 8:43 PM
So, when i compare to subchains, the altchain which does as alternative should prove to be done some particular amount of hashing operations, so i still think it's about cost of hashing power, and in this case performing long range wold cost way more then just simple fast 51% attack
---
"if I do 1.2 gigahashes per second for 5 hours, I will have computed 3x more hashes in comparison to doing 2 gigahashes per second for 1 hour."
- this just confirm what i'm telling. Cost of ghash/hour are the same, isn't it ?

zack || Yesterday at 8:45 PM
oh, I must have misunderstood something

crypto_zoidberg || Yesterday at 8:46 PM
i'm not good in explanations, sorry if did confused you with something

Jed_T || Yesterday at 8:58 PM
think i can say for many, Both of you did very well in explaining things, Thank you to both of you for taking the time today i hope we have more discussions like this in the future :100: :beers:

Shea (UTC+1) || Yesterday at 9:01 PM
Good day in crypto :)

crypto_zoidberg || Yesterday at 9:05 PM
sure, it was pleasure for me to have such an strong and focused reviewer!

zack || Yesterday at 9:06 PM
:)
Thanks for helping me to understand your work