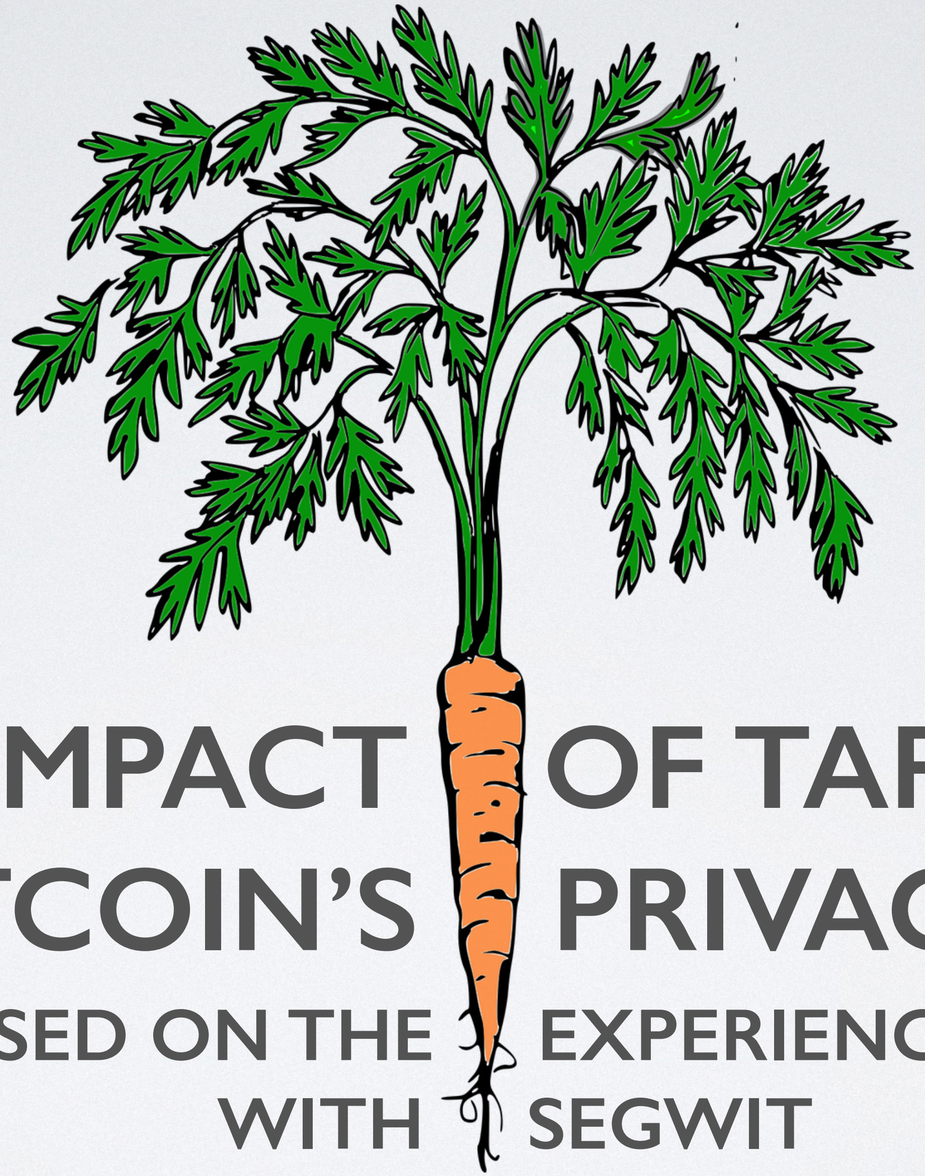


NEGATIVE IMPACT OF TAPROOT ON BITCOIN'S PRIVACY

BASED ON THE EXPERIENCE WITH SEGWIT

https://twitter.com/nikzh

WHAT IS TAPROOT?

- Taproot is a proposed upgrade to Bitcoin that would allow "privacy preserving switchable scripting". It includes BIP 340 (Schnorr Signatures for secp256k1), BIP 341 (Taproot: SegWit version 1 spending rules), and BIP 342 (Validation of Taproot Scripts).

- Taproot needs to be activated by miners. One of the goals of this presentation is to urge miners to thoroughly examine Taproot's implications for Bitcoin's privacy before voting in favour of this upgrade.

WHAT IS TAPROOT?

- Amongst many things, it implements a new standard script (address) type — P2TR. As of today, Bitcoin has multiple standard script types: P2PKH (addresses starting with "1"), P2SH (addresses starting with "3"), P2WPKH and P2WSH (two different types starting with "bc1"). P2SH was introduced in 2012, P2WPKH and P2WSH were introduced in 2017 along with SegWit. SegWit also created some additional awkward constructs, such as "P2SH-P2WPKH", allowing for backwards compatibility, as it was a soft fork.

WHAT IS TAPROOT?

- While Bitcoin Core developers argue that Taproot will increase the privacy of Bitcoin, we cannot agree with that. It certainly may bring something new for experienced users, but for the average Bitcoin user it will only degrade the overall privacy level by a lot.

- The main reason Taproot will degrade privacy is the addition of a new address type.

- We will prove that adding new address types leads to a privacy degradation taking SegWit as a notorious example.

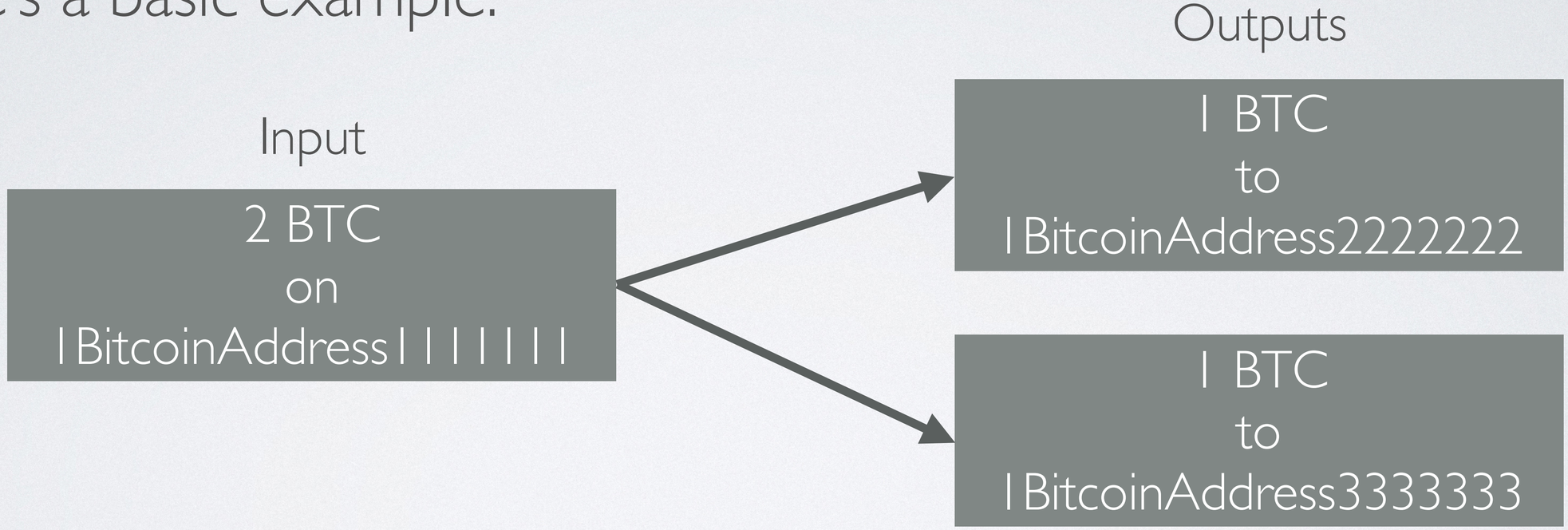
HOW DO MULTIPLE ADDRESS TYPES DEGRADE PRIVACY?

- In most cases when you transact on the Bitcoin network, you'd need to create a transaction with two outputs — one for the recipient, and one for yourself — known as a change output.

- This is because Bitcoin utilezes the UTXO model. If you previously received 2 bitcoins and want to spend just 1, you can't split them in half — you'd need to spend it wholly, creating 2 outputs: 1 bitcoin for the recipient, and 1 bitcoin back to yourself.

HOW DO MULTIPLE ADDRESS TYPES DEGRADE PRIVACY?

- Here's a basic example:



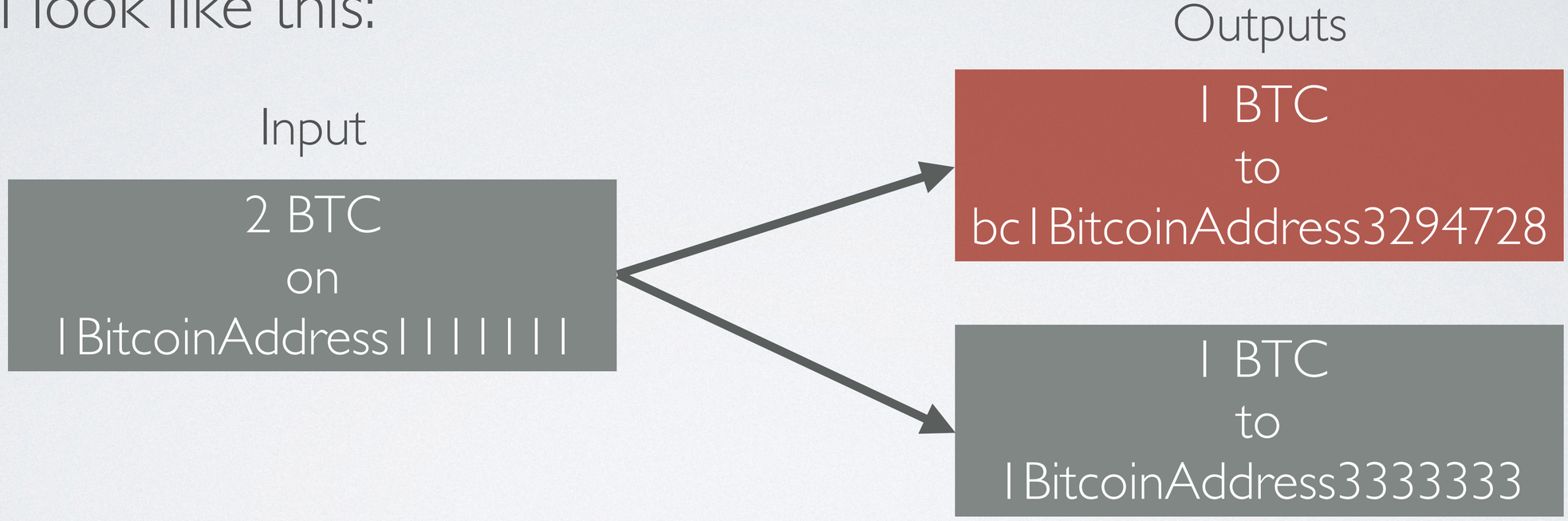
Note that here we can't say which output address belongs to the recipient and which one is the change address.

HOW DO MULTIPLE ADDRESS TYPES DEGRADE PRIVACY?

- Now imagine that the recipient has upgraded to SegWit and is now using the native SegWit address format (starting with "bc1").
- The sender's wallet continues to create change addresses of the same type as it had initially done (starting with "1").

HOW DO MULTIPLE ADDRESS TYPES DEGRADE PRIVACY?

- It will look like this:



Now an analyst can ascertain that 1BitcoinAddress1111111 and 1BitcoinAddress3333333 belong to the same person (the sender)! This allows address clustering which is a potential security risk for both the sender and the recipient.

HISTORY OF UPGRADES

- The first upgrade to add a new address type was P2SH.
- Then SegWit added P2WPKH and P2WSH.
- The planned Taproot upgrade will add P2TR if activated.
- … now let's see in detail how privacy has been degraded with each upgrade!

SCENARIOS: JUST P2PKH ADDRESSES

	Exchange P2PKH
User P2PKH	OK

Here's the default scenario pre-P2SH activation: everyone mostly uses P2PKH addresses (of course, we should keep in mind that there are also P2PK outputs and native multisig scripts, but these were not widely used). No privacy leaks in this case!

SCENARIOS: P2SH IMPLEMENTED AND USED FOR MULTISIG BY SOME EXCHANGES

	Exchange P2PKH	Exchange P2SH
User P2PKH	OK	BAD

Now we introduce P2SH and we can already see a reduction in the privacy level here. If an exchange uses multisig P2SH addresses, it automatically makes all transfers to this exchange transparent for analysts. Note: most ordinary users have no reason to use P2SH, so we don't include that case here, leaving it for exchanges only.

SCENARIOS: NATIVE SEGWIT IMPLEMENTED AND USED BY BOTH SOME EXCHANGES AND SOME USERS

	Exchange P2PKH	Exchange P2SH	Exchange P2WPKH	Exchange P2WSH
User P2PKH	OK	BAD	BAD	BAD
User P2WPKH	BAD	BAD	OK	BAD

With the activation of SegWit, the situation further deteriorated. Now users also have two options, as they may want to save in fees with SegWit, and exchanges have four options. Only if both the user and the exchange use the same address type, will an analyst be unable to exctract valuable information.

SCENARIOS: TAPROOT IS ACTIVATED AND USED BY BOTH SOME USERS AND SOME EXCHANGES

	Exchange P2PKH	Exchange P2SH	Exchange P2WPKH	Exchange P2WSH	Exchange P2TR
User P2PKH	OK	BAD	BAD	BAD	BAD
User P2WPKH	BAD	BAD	OK	BAD	BAD
User P2TR	BAD	BAD	BAD	BAD	OK

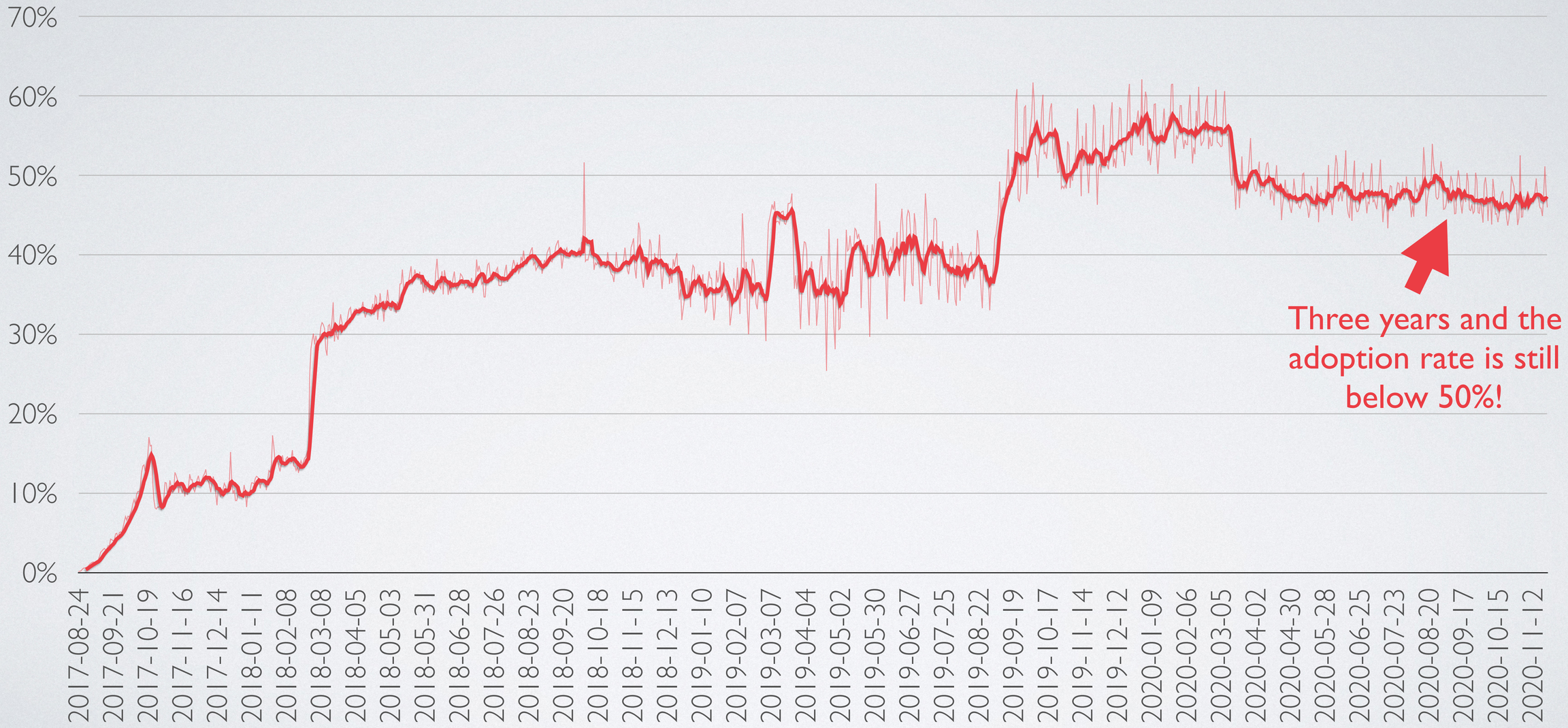
Taproot makes things super bad in that regard. Now there are 15 scenarios in total, and only 3 are acceptable privacy-wise.

AN IMPORTANT NOTE

- Those who advocate for Taproot and deny its negative impact on privacy imply that everyone will be using Taproot, so it will come down to the safe "every user uses P2TR, and every exchange uses P2TR" scenario in no time.

- Unfortunately, this is utopian. More than 3 years since the activation of SegWit and it is still used in less than 50% of all transactions (see the chart on the next slide). It's just not enough.

SEGWIT ADOPTION IS NOT GOOD ENOUGH!



https://twitter.com/nikzh

SO…

- It's been 3 years and SegWit adoption is still under 50% despite economic incentives.
- There's no reason to believe that this number will be better for Taproot, especially considering the incentives are even worse! Let's discuss this in more detail.

WHY WILL IT BE EVEN WORSE FOR TAPROOT THAN IT WAS FOR SEGWIT?

- There's been a very active campaign since 2017 to push users to either upgrade their nodes, or to switch to a wallet that supports SegWit.

- Unlike Taproot, SegWit provided an economic incentive for users — it lowered transaction fees for those who upgraded! Taproot doesn't do this (see the table on the next slide).

WHY WILL IT BE EVEN WORSE FOR TAPROOT THAN IT WAS FOR SEGWIT?

	Default (P2PKH)	Wrapped SegWit (P2SH-P2WPKH)	Native SegWit (P2WPKH)	Taproot (P2TR)
Output size (single signature)	34 B	32 B	31 B	43 B
Input size (single signature)	148 B	91 vB	68 vB	58 vB

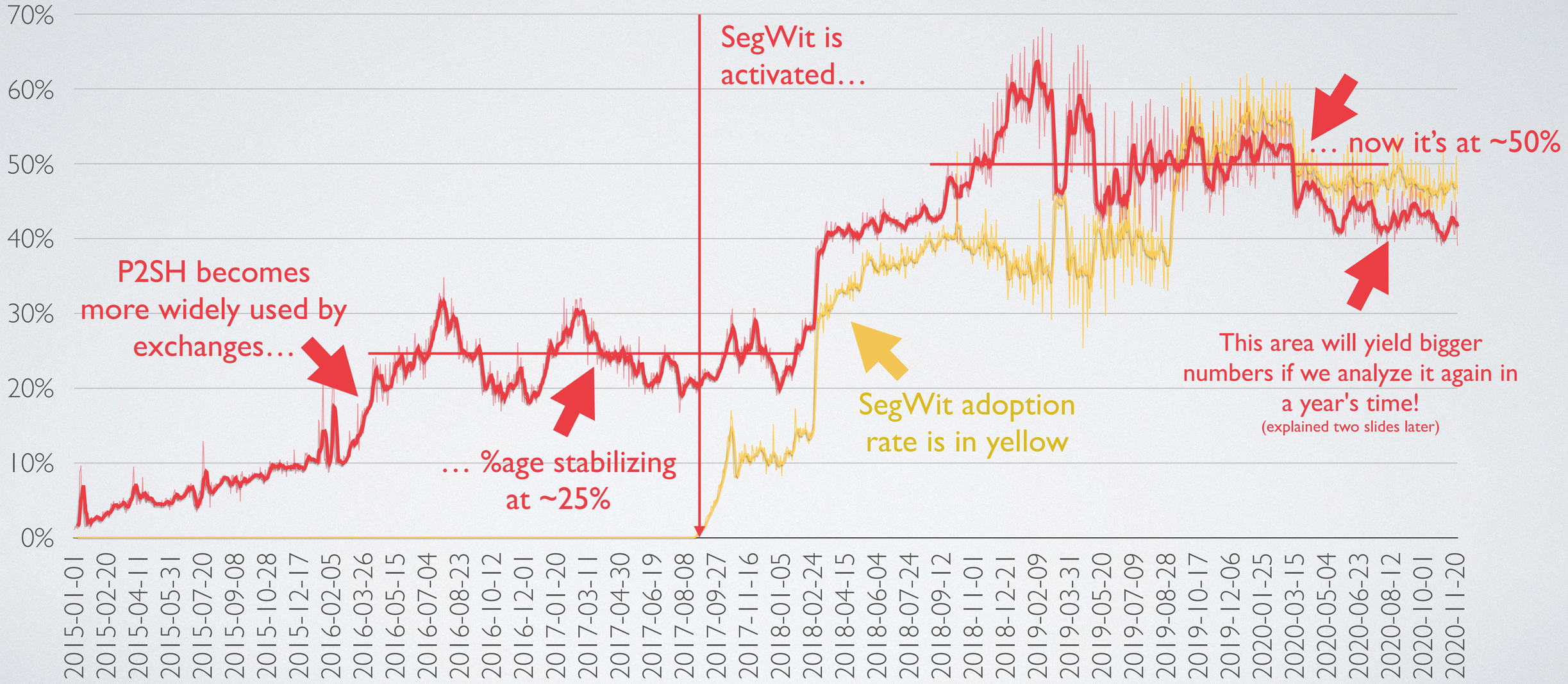
Data source for this table: https://twitter.com/murchandamus/status/1262062602298916865, B are bytes, vB are virtual bytes

- As you can see, SegWit improved things (the smaller the size, the less you pay in fees). P2TR outputs are actually more expensive to create, though they're less expensive to spend. So one may be economically incentivized to accept payments using P2TR. But, compared to what SegWit offered, the savings are miniscule.

LET'S FINALLY MEASURE HOW BAD IT IS

- Let's analyze how SegWit affected Bitcoin's privacy and use that information to project the impact of Taproot.
- To do so, we'll analyze the entire Bitcoin blockchain. We'll look into every transaction (almost 600 million!) and see whether an analyst can extract something useful based on address types.
- We'll be using databases from blockchair.com as the data source, but anyone tech-savvy with lots of free time (a scarce resource!) can run the same analysis using a full Bitcoin node.

PERCENTAGE OF TRANSACTIONS EXPOSING THE RECIPIENT/ CHANGE ADDRESS DIFFERENTIATION DUE TO ADDRESS TYPES USED



https://twitter.com/nikzh

PERCENTAGE OF TRANSACTIONS EXPOSING THE RECIPIENT/ CHANGE ADDRESS DIFFERENTIATION DUE TO ADDRESS TYPES USED (DISCUSSION)

- We clearly see that once SegWit was activated and started to be adopted more and more, the amount of transactions that leak sensitive data to analysts, because of different address types, has doubled from 25% to 50%!

PERCENTAGE OF TRANSACTIONS EXPOSING THE RECIPIENT/ CHANGE ADDRESS DIFFERENTIATION DUE TO ADDRESS TYPES USED (DISCUSSION)

- Small note: using the same method, we've also analyzed P2SH subtypes, including the "P2SH-P2WPKH" nesting doll, and multisig types. That can be done only once these outputs are spent. So if we run the same analysis in a year, given that the older outputs are more likely to be spent, we can expect the numbers to increase slightly on the left side of the chart, and a little more on the right side.

ONE MORE (IMPORTANT) THING!

- Previously we've been talking only about an indicator that allows the differentiation of the sender address from the change address. But obviously, there are more indicators analysts use!

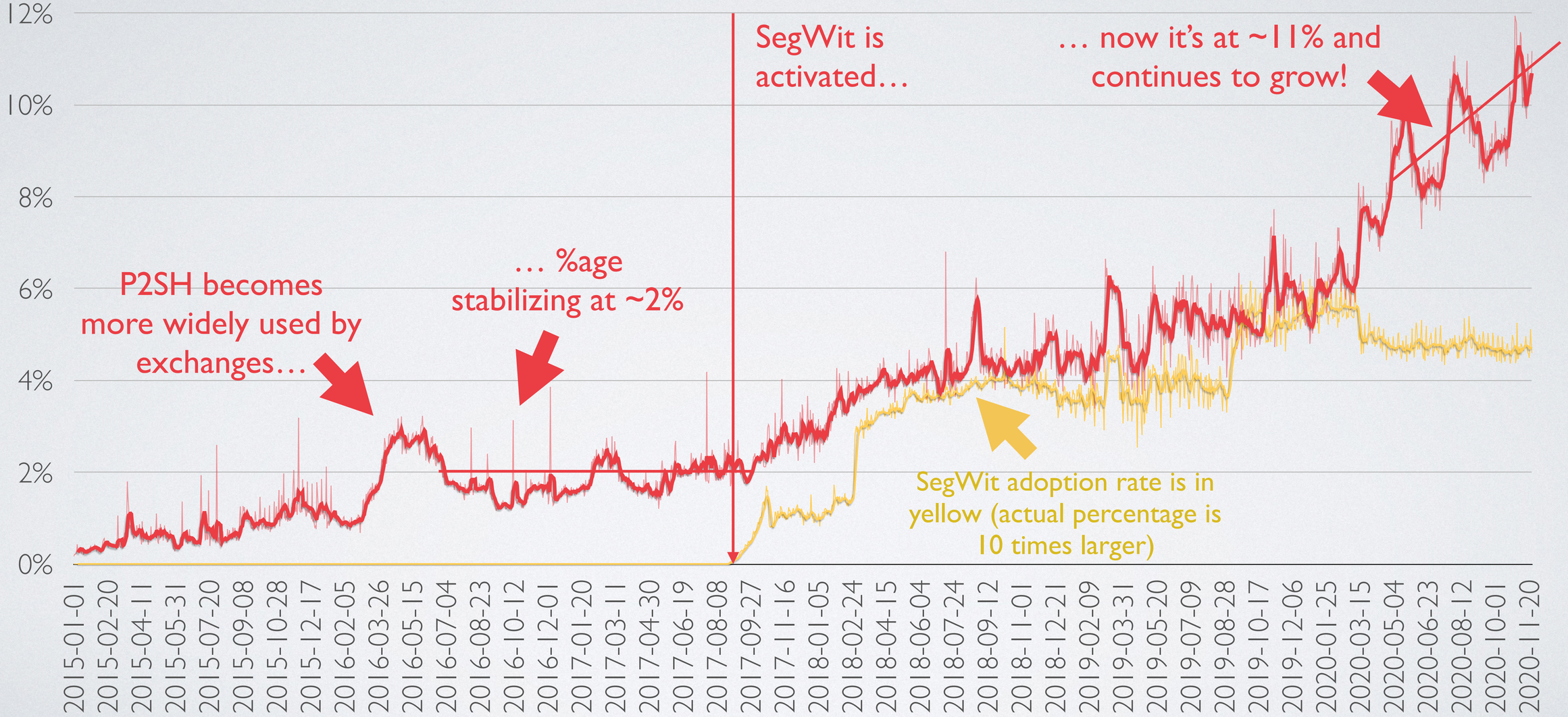
- One of these heuristics is "sweep to another address type". It happens when user migrates to a new wallet (e.g. to use SegWit) — they consolidate their entire UTXO set in one transaction. So these are 1 output transactions (no change) where all inputs are of one type (e.g. "lecacy" P2PKH), and the output is of another type (SegWit's P2WPKH).

ONE MORE (IMPORTANT) THING!

- Unlike the previous indicator where it's hard for a user to evade tracking (let's presume they can't ask every recipient to give them the address type they need), sweeping funds into another address type is a user error (well, not an error, but shortsightedness).

- But actually, Bitcoin Core developers are pushing users to do this! How many times over the years have you seen "switch to a SegWit-compatible wallet to save on fees" from various "experts" who don't care about privacy?

PERCENTAGE OF "SWEEP TO ANOTHER ADDRESS TYPE" TRANSACTIONS



https://twitter.com/nikzh

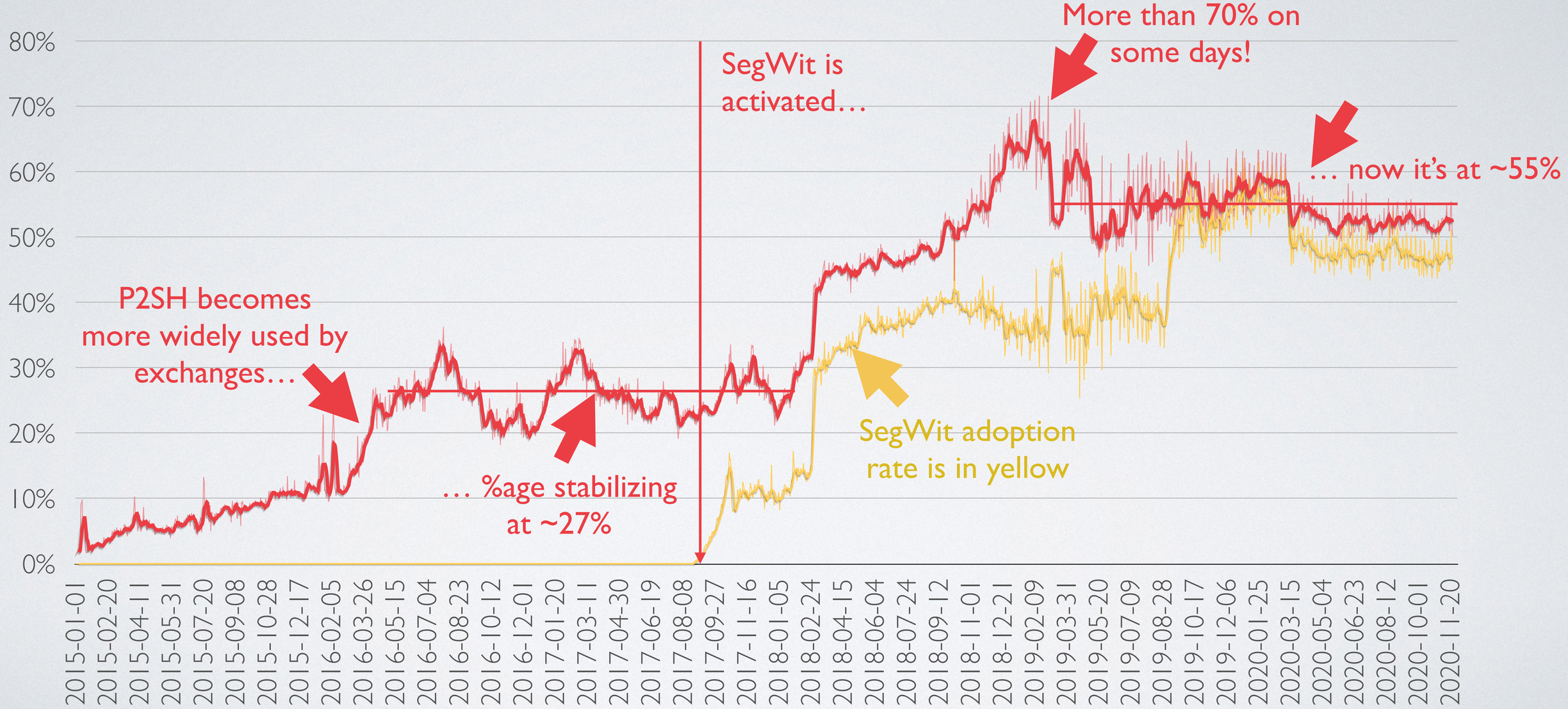
PERCENTAGE OF "SWEEP TO ANOTHER ADDRESS TYPE" TRANSACTIONS (DISCUSSION)

- Once again, we see that once SegWit was activated things started to worsen rapidly!
- The "switch to SegWit" marketing campaign has had a disastrous effect on users' privacy.
- Note: obviously, not all of these transactions are user sweeps to a new wallet type, these may also be "send all my funds to a casino that doesn't support my address type, so I'll lose both my money and privacy". But these transactions can be clusterized as well.

- Minor note: data for 2015-07-09—2015-07-13, 2015-08-01, 2015-09-11—2015-09-18 periods is smoothed out due to some anomalous transactions on these days.

NOW LET'S SUPERIMPOSE THESE TWO CHARTS AND SEE THE TOTAL DAMAGE TO PRIVACY SEGWIT HAS DONE BY BRINGING NEW ADDRESS TYPES!

GENERAL CHART: PERCENTAGE OF TRANSACTIONS THAT LEAK METADATA DUE TO NEW ADDRESS TYPES INTRODUCED BY SEGWIT



https://twitter.com/nikzh

GENERAL DISCUSSION

- As we can see, **SegWit has sufficiently worsened the overall Bitcoin privacy level** by allowing analysts to spy on users' transactions using just two simple indicators!

- Before SegWit, these indicators allowed the gathering of metadata on 27% of transactions. Right now it's over 55%, reaching more than 70% on some occasions! An increase of twofold!

GENERAL DISCUSSION

- As we've previously discussed, there are no signs that Taproot's adoption will be better than SegWit's.
- Not only is Taproot a problem, but SegWit also remains a problem! And the Taproot+SegWit duo will multiply the damage, as there will be more address types in use at the same time!
- As we can't forecast Taproot's exact adoption numbers, we can only speculate that **the precentage of transactions that have privacy leaks because there will be so many address types will rise to 80-90%** if everyone uses different address types — that will be a disater for Bitcoin's privacy!

SUGGESTIONS

- As Taproot is activated by miners rather than developers or exchanges, miners are strongly advised to run their own analysis and **block the Taproot upgrade**!

- Miners should also think about other implications of Taproot and SegWit! One of the main reasons the Bitcoin Core developers are pushing for these upgrades is that these new functions are required to build new (mostly centralized) layer 2 solutions which will siphon fees away from miners (that's a topic for a different presentation though).

WHY IS NO ONE TALKING ABOUT THIS?

- You may be asking yourself "why is it only some no name Nikita who is against Taproot" and that would be a valid concern!
- The answer is quite simple: most of those who are able to run this kind of analysis have some conflict of interest. I do not.

WHY IS NO ONE TALKING ABOUT THIS?

- Bitcoin Core developers (and associated for-profit companies like Blockstream, Chaincode Labs, etc.) need Taproot for their new products: a clear conflict!

- Forensics tools developers (like Chainalysis or CipherTrace) obviously know about these privacy downsides, but they're more than happy about that as it makes their job easier!

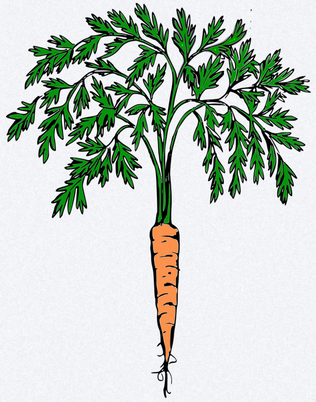
- We'd speculate that there are many institutional entites that may be aware of the issue, but they're interested in Bitcoin being as transparent as possible, thus it's better for them to help forensics companies, rather than the average Joe.

WHY IS NO ONE TALKING ABOUT THIS?

- And actually there are others (not a lot yet though):
  - http://blockchain.cs.ucl.ac.uk/wp-content/uploads/2020/04/UCL_CBT_DiscussionPaper_Q12020_Anania_2020.pdf (the authors seem not to have any conflict of interest)
  - … and even one of the Taproot developers talks about this at its presentation: https://www.youtube.com/watch?v=YSUVRj8iznU&feature=youtu.be&t=2097 (34:57 mark)

THANK YOU!

And don't forget: **BLOCK THE TAPROOT UPGRADE**, IT IS NOT TOO LATE!
Please help to spread the message to miners and follow me on Twitter for further updates.



https://twitter.com/nikzh