21 tweets about the scaling debate

scritto da Alberto De Luigi | 4 Giugno 2017
You can follow the stream on twitter ***here***

1/segwitx2 won't cause a drop in full nodes numbers. It's economically sustainable for worldwide average users who want to run a full node

2/..and will be more sustainable as technology improves. There are no serious centralization issues with Silbert accord

3/segwit2x is no bowing to miners' blackmail, just the anticipation of something needed (2mb HF) as stated in Core roadmap:

4/"advances in technology will reduce the risk and therefore controversy around moderate block size increase proposals"..

5/…we "will be able to move forward w/ these increases when..their risks widely acceptable relative to the risks of not deploying them"

6/Core dev Matt Corallo says about segwit2x he is "totally supportive of the stated goals" ***see here***

7/After LN release, we need low onchain fees if we want it to be decentralized, 2mb block increase might be helpful. I exemplify:

LN.1/Alice receives a 2btc payment from Mallory, intermediary is Bob. Last commitment tx in Alice-Bob channel has balance: A,B(5,5).

LN.2/in A-B channel a new commitment created: A,B(7,3). Alice can broadcast onchain only if she knows Image from Mallory.

LN.3/a new commitment is created in channel B-M, previous balance B,M(10,5) now (12,3)

LN.4/Mallory gives Image to Alice. She broadcast onchain. Mallory broadcast the past commitment B,M(10,5) onchain, at her own risk

LN.5/Bob is distracted or for whatever reason can't broadcast the Breach Remedy tx (15,0). Mallory stole Bob money.

LN.6/Bob has a risk to act as intermediary. The higher the risk, the higher the fee.

LN.7/Indeed, LN will have low fee, because it will be software, not Bob, that broadcasts Breach Remedy tx

LN.8/But when will be released nice GUI safe (or SPV smartphone) software to allow avereage users for LN payments? Months? Years?

LN.9/When LN will be ready, if average users have to pay very high fee for onchain tx, there won't be a very capillar network

LN.10/Rather, only main wallet providers will act as intermediaries. When a user deposits btc in the wallet, he will already open a channel

LN.11/the wallet provider will soon have network advantage. Users prefer a unique intermediary rather than open new channels with onchain tx

LN.12/economy of scale: a few wallet providers will own the quasi-totality of intermediary channels. Oligopoly. Offchain fees increase

LN.13/attacking the wallet provider (the hub) may result in a slowdown of transactions.

LN.14/an attack may also prevent the hub from broadcasting Breach Remedy tx: funds may be stolen?

LN.15/LN is the only way to scale, but needs to be decentralized: blocksize-increase guarantees lower fee onchain and offchain..

LN.16/…such that people can open new channels without high costs: the way to offhchain intermediaries decentralization

8/I think scaling debate is more a matter of ideology than stakeholders interests. But if we want to be mischievous:

9/self interested miners are for bigblock, because onchain fees. Self interested developers are for small block, because offchain fees

10/The cost and benefits of the onchain vs offchain tx actually compete, and miners/devs have interests in lessening competition

11/best scenario for users: sw active and blocksize increasing

as technology improves, on condition that average users able to run fullnodes

12/Be pragmatic and less ideological. The only way is to concede 2mb. UASF not viable unless it reaches 51% hashrate

13/UASF is a SF chain split, sgwit2x a HF with much less probabiliy to cause a split

14/There is no Core support to UASF bip 148 *see here*

15/#UASF: chain split without miners, without developers, without other players like exchanges. And without users. Are u serious?

16/#UASF is more #TNASF than else (Twitter Noise Activated Soft Fork)

17/be very optimistic, UASF chain reaches 20% hashrate; this could be the scenario with parts of the total hashrate mining distribution:

18/non-uasf chain 51%, 20% uasf, 21% non-uasf miners orphaning blocks in UASF chain (if just a part of segwit2x miners hashrate coordinates)

19/If non-uasf miners are really able to coordinate, they can also easily manage a 33% uasf attack (more details if u ask).

20/if the scenario gets more complicated, with counter-uasf hard (or soft) forks, the chain splits will be so harsh..

21/…that you'd be better off moving to Litecoin :)