Hi all,

My first post on this platform. The follow discussion took place this morning in the Telegram Channel on the Open Source Block Explorer. It was requested in the channel to save/continue discussion here. I am seeking corrections, additions, et cetera…

Transcript below:

Griff Green (admin):

Random Q guys: Is there a good way to see if a reorganization happened on Ropston? In our bridge logs from 2 days ago, there's a point where getBlockNumber jumps back 1000+ blocks, I assume its a problem with our node or our code, but we are having trouble finding a way to check if ropsten had issues.

Does anyone know of any tools for visualizing/analyzing reorgs, on ropsten or in general?

Emiel Sebastiaan:

@GriffGreen : Jumping back n-blocks happens in case of a chain reorganization (i.e. a newer longest chain). This should not go unnoticed by Etherscan via page: https://ropsten.etherscan.io/blocks_forked

I know because we at WEB3SCAN had to reproduce this when building our Block Explorer (harvester). The page I mentioned at Etherscan (with the reorgs) is a byproduct if your block explorer needs to follow the tip of the chain and not assume some sort of effective finality like exchanges do (of 12,5 minutes). If your explorer/harvester indexes the tip of the chain then you will notice that quite often you are on some local fragment of the network that (for a brief moment) has a longer chain than the eventual canonical chain. These blocks will later become uncles. The thing is that such functionality in your harvester would detect any minor and major reorganization such as 51% attacks.

That said, apparently what you suggest is NOT visible on Ropsten Etherscan. This may imply it did not happen, but gives no guarantee. Etherscan's node could have been down and thus missed it, or something else altogether… Anyway such reorganization after the fact cannot be assessed by the node alone since it only stores the canonical chain.

Hope this helps!

Emiel Sebastiaan

As a follow-up I would suggest the next bounty on the list for @Mitch_Kosowski

"An event monitoring service for particular type of events that are of value to the community but cannot be detected via straightforward methods such as single nodes (regardless of their mode of operation)." Obviously a full audittrail should be made available by those monitoring services in case of occurence of such events designed and operated by N independent parties.

I can already name two such events that should be actively monitored and all alarm bells should go off when such events occur.

1. Chain reorganization of more than N blocks. (>N blocks to account for normal eventual uncles).

2. Concensus failure between clients.

I suggest any community funded bounty should incentivize N independent parties to design and operate these event monitoring services for one year based on assessment of predefined metrics/events. The requirements can go up for next year/bounty. >N independent parties designing and operating these services allow for extra rigor and cross-validation.

Last but not least. This would be of value to testnets! I urge that testnets will be explicitly included in such bounty!! I know there are concensus algoritm agnostic design patterns to detect chain reorganizations. So even if testnets do not use a PoW mechanisms (Kovan, Rinkeby and many others) one can design detection services of chain reorganizations.

Such event monitoring service requires some old-school Service Management skills. It should be a community bounty, because the community buys itself a more or less fail-safe early warning system.

Hope this helps (made some edits please re-read).

Emiel Sebastiaan

This is a discussion that goes back in this thread and in the broader community. In many cases the standard response of this community for matters of concern or matters where resilliancy is important, is to design a decentralized, trustless, trust-minimized or p2p pattern for such system.

My point perhaps is that such design patterns take quite some time to develop and mature and most importantly are very hard. There is nothing wrong with some good old fashioned design patterns to get some short/medium term value… Furthermore these relatively small bounties may allow for various smaller players to develop platforms that can eventually

really compete with Etherscan or even offer something better.

Mitch Kosowski (admin)

Excellent! Could you please open a thread on Ethereum Magicians or your favorite forum to make sure this discussion doesn't get lost like tears in the rain? And also to bring other interested parties into the conversation