**Ghost protocol**Transactions can be published from anywhere in the network. The role of miners is to collect, verify, and publish these transactions as blocks on the chain. Due to the random nature of the hashing in a proof of work system, it sometimes happens that two blocks are produced by two different miners at around the same time. This results in one of the blocks not being included on the main chain and discarded.

These blocks that are valid but unfortunately not included on the main chain are described as **“orphaned.”** Normally, the miners of these orphaned blocks are not rewarded, and their efforts do not add to the total work of the chain

Then the Ghost protocol (Greedy Heaviest Observed Subtree) was introduced in 2013 for the Bitcoin blockchain and solves for some of the security and efficiency problems currently seen with that and other Proof-Of-Work blockchains.

It is a way of combating the way that fast block time blockchains suffer from a high number of stale blocks - i.e. blocks that were propagated to the network and verified by some nodes as being correct but eventually being cast off as a longer chain achieved dominance, or Forking.

GHOST Protocol adopts some of these orphaned blocks as **“uncle blocks”**and assigns partial rewards to the miners of these blocks, but more importantly, the work from these blocks is also included on the main chain. Including the work from these uncle blocks makes it more difficult for an attacker to overtake the main chain, because their own work can be used against them as uncles to further add weight to the main chain.

In essence, **the hash rate of these miners is more efficiently applied to the stability of the HYCON blockchain network, with the added bonus of faster transaction confirmation and processing time due to shorter block intervals that can be achieved with GHOST.**

*The upcoming GHOST Protocol upgrade does the following:*

*1. Cut the block time from 30 to 15 seconds.*

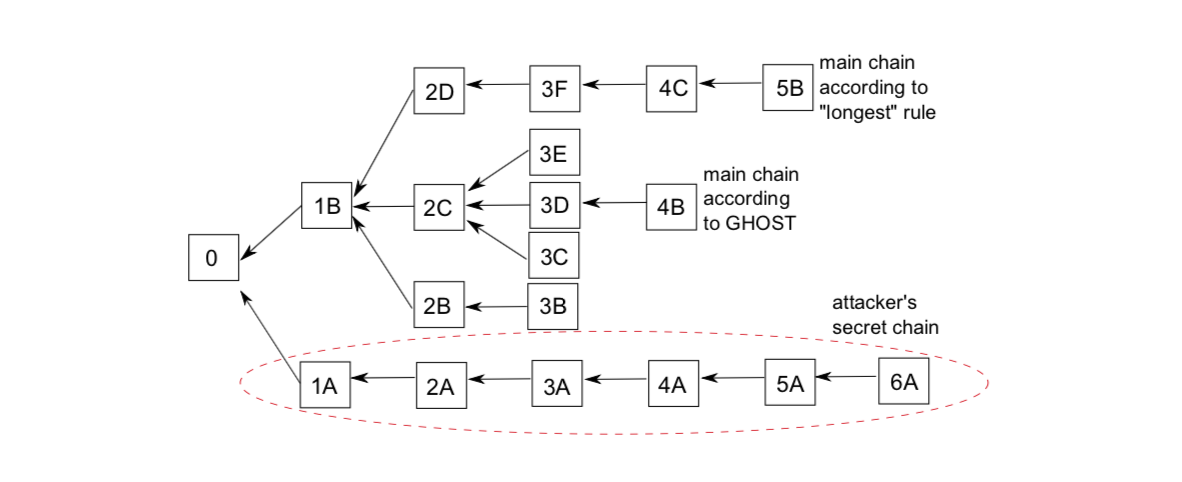
*2. Speeds up the confirmation time as a result of decreased block time*

*3. Reward miners even if they mined a block that is not incorporated in the main chain.*

GHOST includes stale blocks – or Uncles as Ethereum calls them – these are included in the calculation of which chain is longest or has the highest cumulative difficulty. Centralisation is solved by giving block rewards to stales of 87.5% – the nephew (child of the Uncle block) also receives a reward of 12.5% of the block reward.

The Ethereum version of Ghost only goes down seven levels – or back seven levels in the height of the block chain.

* A block must specify its parents and its number of Uncles.
* An Uncle included in a block must be a direct child of the new block and less than seven blocks below it in terms of height
* It cannot be the direct ancestor of the block being formed.
* An Uncle must have a valid block header.
* An Uncle must be different from all other Uncles in previous blocks and the block being formed.
* For every Uncle included in the block the miner gets an additional 3.125% and the miner of of the Uncle receives 93.75% of a standard block reward

****

**In this case, attacker's chain is doomed. so i think one of the problem's chance which is having 51% hash rate power and broadcasting the longest chain has been decreased(which is great). But I still see a couple of issues.**

1. **If blocks don't get mined at the same time, we won't have subtrees as shown on the image, Hence GHOST protocol is powerless here. and we still have 51% attack possibility and in this case, attacker's secret chain will succeed.**
2. **So, if blocks get mined at the same time, that's when GHOST protocol will help us. I guess GHOST protocol is a little bit of extra safety added on top of proof of work. but as soon as nodes followed GHOST protocol(which means, they accepted the chain - from the image it's 0->1B->2C->3D->4B), we are back to where we were(longest chain wins). until blocks start to get mined at the same time again..**

**Pros of GHOST Protocol**

* **Easy transactions:**In a world where cryptocurrency transactions can be completed within seconds from anywhere in the world, GHOST Protocol allows individuals to make transactions with ease through efficient use of computing power.
* **Freedom to developers:** If a developer doesn’t want to take on the responsibility of maintaining their own infrastructure, they can utilize GHOST-powered smart contracts which run on top of it instead.
* **Saves time and effort:**It saves them time and effort. Smart contracts are much quicker and easier than writing applications from scratch. It allows for more people to get involved in the dApp space. This is a great thing for new developers and entrepreneurs to get involved in.
* **Better transparency:**It provides better transparency than Ethereum’s ERC20 standard (which platforms like MyEtherWallet and MetaMask still use). It allows developers to accept payments while being completely anonymous. A non-anonymous or pseudonymous payment system is much preferred by hackers and online phishers, preventing them from either targeting you or stealing your funds.

**Cons of GHOST Protocol**

* **When not in use over-complicated:**If no one wants to use the GHOST protocol, it will remain an over-complicated means of paying users in their tokens or Ether.
* **Not viable option:**It’s not a viable option for certain platforms. Blockchain-based games are the first thing that comes to mind.
* **Gas costs for all transactions:**dApps utilizing this protocol need to pay the gas costs of all transactions, even those that don’t involve them.