Reduction in energy consumption by Ethereum in January 2019

Aman Sharma
University of Paderborn, Germany
https://www.uni-paderborn.de/
aman1@mail.uni-paderborn.de

Abstract

Digital currencies based on decentralized systems that use distributed ledger referred to as block-chain has seen some major evolution in the present decade. It started with the introduction of Bitcoin that now is holding close to 5.8 million users. One such open-source Block-chain based platform is Ethereum which was introduced in the year 2013 uses Ether as its crypto-currency has also gained equal popularity. Consensus protocol is the basis of these decentralized networks which is a method of co-operation, collaboration and coming to an agreement for settlement of transactions. One of the first algorithm for consensus was Proof-of-work used to verify transactions and blocks in the network in which the responsibility is given to each node known as miners to solve a complex mathematical puzzle. This process of mining involves huge computation power and hence tremendous consumption of electricity. Yearly energy consumption of Ethereum network is 75,90,000 Mwh which is even more than the early consumption of Iceland which is alarming. But in January 2019, Ethereum has changed the way to reach consensus that has reduced the energy consumption to 1% of the previous. This report primarily focuses on the new Ethereum's proof-of-stake algorithm called Casper, implemented to save energy and also improving the security as a bi-product of this change.

2012 ACM Subject Classification

Keywords and phrases Ethereum, Consensus Protocol, Proof-of-Work(PoW), Proof-of-Stake(PoS)

Digital Object Identifier 10.4230/LIPIcs.PotB.2020.3

1 Problem Description

1.1 High Energy Consumption

It is worth mentioning that most of the analysis in the crypto-currencies world is done majorly on the consensus mechanism and how to make them more secure, rather very less efforts have been put on the analysis of energy consumed during mining process. There is no clear-cut method of estimating the energy consumption during the mining, though one possible estimate could be given by multiplying the energy consumption of the most efficient miner with the total network's hash-rate. This absolute value is pretty optimistic as we are considering the minimum of energy consumed by all the miners which gives us the best case scenario, on the other hand energy spent by the least efficient miner can be taken to estimate the worst case.

Mining process requires high end CPUs to solve computational puzzles and the first such Ethereum specific mining device called Ethereum ASIC (Application Specific Integrated Circuit) was introduced in 2018. But their introduction to the Ethereum network has been criticized by many experts because high efficiency of these devices can lead to the creation of mining farms, promoting centralization which may ultimately lead to the devaluation of Ether. As most of the Ethereum mining is done in a traditional way using Graphics Processing Units (GPUs), some of the most power-efficient GPUs, NVIDIA GeForce GTX 1070(150W per unit) and Nvidia GeForce GTX 1060 with 120W per unit are least power-hungry[3] and

Ethereum's Total Network Hashrate in GH/s is 161,474.00[1]. The product of these two figures gives us an estimate of the energy consumed by the network.

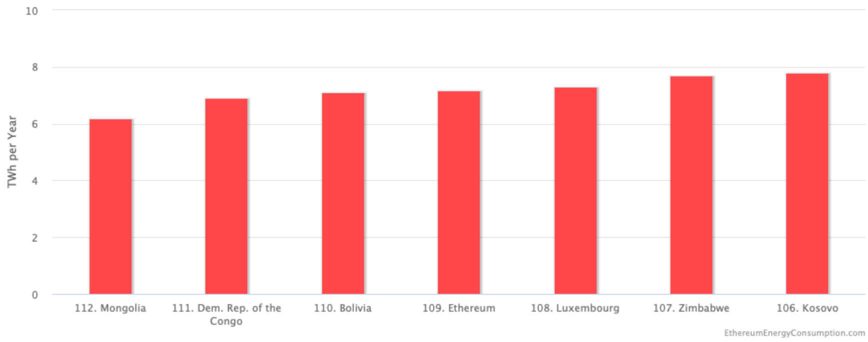

Figure 1 Ethereum Energy Consumption by Country[1]

One such analysis is done by an organisation called Digiconomist which does analysis of digital trends from the economic perspective, and it states that the Ethereum's Energy consumption in the month of November, 2018 was 19.84 TWh (see figure 2). Furthermore, if compared with the annual power consumption of some of the countries, Ethereum consumes just less than the whole state of Luxembourg and Zimbabwe analysed by EthereumEnergyConsumption.com (see figure 1). But other payment processing systems like VISA respectively MasterCard consumes roughly 0.00092 khW and 0.00070 Kwh per transaction [6] as compared to 37 KWh by Ethereum.

Figure 2 Ethereum Energy Consumption Index Chart in November 2018[1]

1.2 Risk of Centralization

Proof-of-work gives higher rewards to the miners with better or high-end equipment. Chances of creating the next block and thus, receiving the mining rewards increases depending upon the miner's hash rate. In Proof-of-work, investment in setting up massive equipment and the energy wasted is not linear as high energy consumption does not necessarily yield linearly high price i.e. for 1 KWh of electricity if 1$ is earned does not mean 1000 KWh will yield 1000 $.

Nevertheless, miners can come together to form a 'mining pool' which increases the chance of centralisation even further and the received awards can be distributed evenly among each node in the pool. This leads to two major issues: excess energy consumption and centralization of the block-chain, thus, opposing the fundamental idea of decentralization. It is worth noticing that the mining groups can also decide the fortune of a block-chain network (see figure 3) if top three mining groups (constituting more than 50% of the nodes) combine together they can effortlessly take control of the transactions in a network.

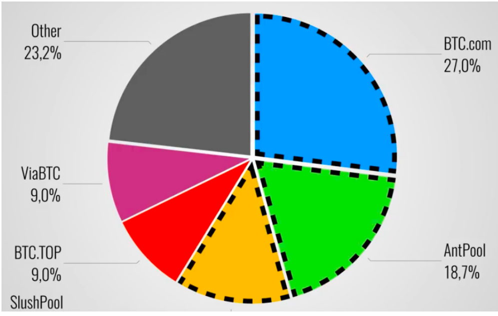

Figure 3 Pooling Groups [2]

Thus, in a race to create a next block in the chain, these big centralized mining farms and other miners burn an excessive proportion of energy. Another main issue arrives when the number of miners (and hence the energy consumption) increase even though the rate of block addition would still remains 10 minutes per block. This means that the speed of processing and the number of transactions remain same and the same result can even be achieved with less miners as well. Furthermore, the addition of more miners increase the unnecessary competition among each other and waste energy which could be saved . In the next section, let us discuss an approach followed by Ethereum to cope up with this issue.

2 Proof of stake - an Alternative Approach to Mining

The main idea of proof-of-stake algorithms is that mining is a wasteful process as miners are indirectly competing against each other, instead the same can be achieved by voting as one node can be randomly elected to validate the next block in the chain. It focuses on the idea of removing physical processing devices and using virtual Ether in place of them for validating the next block in the chain. As, the chances of validating next block is proportional to the amount of Ether one puts at stake. PoS relies on penalties instead of rewards for securing the transactions. Proof-of-stake has *'validators'* in place of *'miners'* who mint/forge new blocks instead of mining. Although, the process of choosing the next validator can be completely random, but to take part in becoming a validator each node deposits part/ or whole of its collected *ether* into the network as stake. Stake acts as a security deposit and the chances of validating the next node increases for the node with the higher stake.

The problem of trusting a validator is solved if the stake deposited by the validator is higher than the sum of all the validated transactions' fees because if found suspicious by validating fraudulent transactions, a validator may lose his entire stake. In short, the trustworthiness of a node is judge by its amount of stake invested to participate in the election process and by satisfying the aforementioned condition (stake being higher than the sum of the validated transactions' fees), network can build a trust on the validators to do their job honestly.

In order to validate a block, a *forger* combines its public key with the ID of the previous block to seed a random number. This random number is multiplied by their stake and the time since the last block was added (in seconds) and if it exceeds a threshold value, the validator can add the next block into the chain.[2] The voting power of each validator is decided by the amount of ETH they put at stake. Initially, the minimum stake required to participate in the election process to become a validator is 1500 ETH worth $1,065 U.S. Dollars making it hard for an average person to take part in validation process, but in future, this value is estimated to be 32 ETH[5].

The above-mentioned approach cuts the number of processors working to validate a single transaction to just one. This also solves the problem of excessive miners as it disincentivizes the transaction validation process, though some transaction fees is still payed to the validator/ forger for validating the next block in the chain. This is exactly opposite of PoW which relies heavily on the high rewards generated through mining at the cost of massive amounts of power which is undesirable in the present world of global warming. But in PoS, not anyone who has computation power can become a validator unless he puts some stake in the network and the solving of complex mathematical puzzles is also not required. As a result, the number of validators would be less (as compared to PoW) leading to less energy consumption.

3 Casper Friendly Finality Gadget

There have been two co-developed Casper implementations in the Ethereum ecosystem: Casper CBC (Correct-by-Construction) and Casper FFG (Friendly Finality Gadget). This report focuses on the working of Casper FFG which is followed by Ethereum[4]. The term *finality* means that the operations are irrevertible i.e. operations once committed cannot be modified. With Casper's proof-of-stake comes accountability as the system can punish the malicious validator and each validator is accountable for his actions and, thereby enhancing the security.

The current Casper implementation is a hybrid PoW/PoS model as it uses the PoW proposal mechanism but is planned to be changed in future to a complete PoS based system (according to Ethereum's co-founder)[4]. Meanwhile, Ethereum has also decided to stop PoW mechanism completely by increasing the complexity of the mining puzzles to make it difficult to mine blocks thus leading to *'Ethereum's Ice Age'*. This process is termed as dropping a *'difficulty bomb'*[5]. This step tries to eliminate the use of mining and thus reduces the computation and energy used to reach consensus. The following sub-sections describe the fundamentals of Casper FFG.

3.1 Checkpoint tree

Similar to PoW, the first block in the chain is called *'genesis block'*. But unlike PoW, Casper maintains a sub-tree of checkpoints called checkpoint tree(see figure 4). A checkpoint tree is built out of the Ethereum block-chain by taking only the blocks which are the exact multiple of 100 (genesis block is a checkpoint). Thus the height of a block in this tree is simply the checkpoint height of that tree. For Example, a block at height 300 in the actual chain is at height 3 in the checkpoint tree.

3.2 Dynamic Set of Validators

At any point of time, an existing validator can leave and correspondingly new validators can enter the network. Anyone who wants to become a validator or wants to leave the set must include a *deposit* message or a *withdraw* message respectively in the block located at *dynasty d*. The dynasty of a block is the number of finalized checkpoints in the tree starting from genesis block to that block. The block after sending the message can join or leave the set

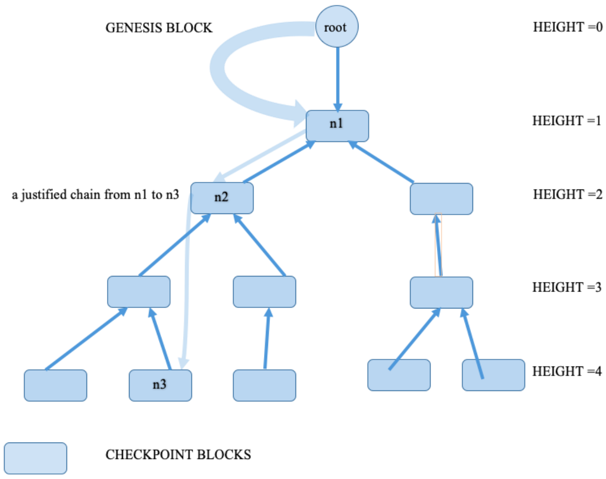

Figure 4 Checkpoint tree

at first block with dynasty d+2. If a validator v joins the set, then d+2 would be called a *'start dynasty' DS(v)* of that validator and if it leaves it would be referred as *'end dynasty' DE(v)*[4].

3.3 Voting Incentives

A validator is rewarded only if the checkpoints are achieved. If a validator does not take part in the voting process, its balance is reduced by imposing certain penalty. The validator who has voted correctly will get positive rewards and the rate of interest depends upon factors like behaviour of the voting and performance of the protocol as a whole[8]. Likewise, the protocol takes no notice of the voters who have voted wrong and are not given any incentive. But, if found guilty of casting a mischievous vote, the entire deposit of a validator can be reduced to zero and the respective account can be removed permanently also referred to as *slashing*. In case of unreachable checkpoint, the correct voter's account remain same.

3.4 Fork Rule

To understand the Casper's fork choice rule, it is important to know few more concepts related to the checkpoint tree. The first and the foremost term is a *super-majority link* written as x $\rightarrow$ y is an ordered pair (x,y) of checkpoints which has received 2/3rd votes of the validators saying x is a source and y is a target[4]. Checkpoints are conflicting if they belong to the different branches. A checkpoint is referred as justified if either it is a genesis block or there exists a super-majority link to that checkpoint from a justified checkpoint. Lastly, a finalized checkpoint is the one which is either a genesis block or it has a super-majority link to its successor in the tree. On encountering a fork, casper chooses the chain which contains the highest justified checkpoint.

4 Limitations

4.1 Problem of Double-Spending

As described earlier, validators try to achieve a threshold to add a new block into the chain, it may happen that two validators reach the threshold at the same epoch leading to two authorized blocks. As, no resources are being burned to forge the next block, one may start forging both the chains to earn more fees. Let us consider a scenario where there are two different chains c1 and c2 from a fork, and 99% of the nodes are doing multi-branch forging by validating blocks in both the chains c1 and c2 for the sake of earning more fees. Now, the remaining 1% nodes decide to put their transaction in chain c2 and after getting the confirmation, they again put their transaction into the other chain c1, eventually giving rise to double-spending the money.[2] PoS is more prone to double-spending because the adversaries need to conquer only the nodes who stake on the original chain (which would be too less in this scenario). Though such attacks are theoretical till now and have never happened, mainly because the mining software would not have the provision to mine multiple forks.

4.2 Biased Approach

As discussed earlier, the chances of validating the next block increases if a validator has more Ether at stake as both are directly proportional to each other. That means if there are 100 Ether coins in the system and a validator A holds 30 Ether out of that his chance of generating next block is 30% but a validator B having 0.5 Ether has only 0.5% chance. Things get worse in the subsequent runs, when A keeps on generating more blocks because of its higher stake, increasing the gap between A and B. It is worth mentioning that with 10,000,000 $USD worth Ether one has just 0.03% chance of solving the next block[7].

5 Conclusion

This report presented the energy consumption rate of Ethereum block-chain network with proof-of-work consensus protocol used earlier than January 2019. Since, block-chain itself is not energy inefficient as it just verifies digital signatures in transactions, but it is the Proof-of-work's mining process that makes it energy inefficient. Ethereum decided to change their consensus mechanism from proof-of-work to proof-of-stake. In spite of limitations, an implementation of Proof-of-stake consensus mechanism called Casper brought a change in the security as well as saved 99% of the power consumption of the Ethereum's whole network.

References

1 *Ethereum Energy Consumption Index. https://digiconomist.net/ethereum-energy-consumption.* URL: `https://digiconomist.net/ethereum-energy-consumption`.

2 *Proof-of-Stake(v/s Proof-of-work).* URL: `https://www.youtube.com/watch?v=M3EFi_POhps`.

3 *Best GPU for Mining–Top 6 Choices. https://www.bitdegree.org/tutorials/best-gpu-for-mining/.* January 22nd,2020. URL: `https://www.bitdegree.org/tutorials/best-gpu-for-mining/`.

4 Vitalik Buterin and Virgil Griffith. *Casper the Friendly Finality Gadget. https://arxiv.org/pdf/1710.09437.pdf.* Ethereum Foundation, 22 JAN, 2019. URL: `https://arxiv.org/pdf/1710.09437.pdf`.

5 Tim Falk. *Ethereum's Casper protocol explained in simple terms.* 6 February 2020. URL: `https://www.finder.com/ethereum-casper`.

6 Amir Abbaszadeh Sori. Green iota, measuring iota pow 's energy consumption and comparing with other payment systems, Aug 16, 2019. URL: https://medium.com/a.abbaszadeh.s/measuring-iota-pow-s-energy-consumption-and-comparing-with-other-payment-systems-413f4de50274.

7 Patrick Thompson. *Is a PoS consensus algorithm fair?* 09 April 2019. URL: https://cointelegraph.com/news/is-serenity-the-solution-to-ethereums-difficulty-bomb.

8 Stefanos Leonardos Georgios Piliouras Ethereum Foundation Singapore University of Technology Vitalik Buterin, Daniel Reijsberge and Design. Incentives in ethereum hybrid casper protocol, 11 March 2019. URL: https://arxiv.org/pdf/1903.04205.pdf.