Project Midterm Report: Exploration of Environmentally Friendly Blockchains

Huangyin Chen, Jianjia Yu, Ziming Chen

I. Introduction

Traditional blockchain with Proof-of-Work as the consensus algorithm requires a huge amount of computing power to work out the puzzles, which translates to enormous energy consumption. In [1], the annual energy consumption involved in mining was estimated to be over 100TWh in total by PoW Cryptocurrencies with the top 5 market capitalization. They determined electricity consumption to be between 60 and 125 TWh per year for Bitcoin. This is in the range of the annual electricity consumption of countries such as Austria (75 TWh) and Norway (125 TWh). As said in the paper, competition in the mining hardware market, resulting from the hype around cryptocurrencies, has dramatically increased the energy efficiency of mining hardware in the last decade.

Building environmentally friendly blockchains is a vital problem we need to think about for the sake of our environment and also for the long-term development of blockchains. In terms of measuring how environmentally friendly the blockchain is, we take into account the energy cost and the hardware cost. We also analyze and compare different consensus algorithms in detail as they essentially determine how much computing power and what kind of hardware will be needed. Moreover, we've made a significant amount of work on grabbing the specific energy consumption data including the annual total electrical energy, annual carbon footprint, and energy cost per transaction of the 2 most popular cryptocurrencies in the world: Bitcoin and Ethereum. We will give a comprehensive analysis of the data and further analyze the possible change of their energy consumption in the future.

II. Consensus Algorithms Overview

The energy cost of blockchain with different consensus algorithms is different due to their different approaches to reaching a consensus. In this section, we are going to present three major consensus algorithms in blockchain, namely, PoW, PoS, and PBFT.

As stated in [1], the blockchain algorithms can be divided into two groups: The first group of consensus algorithms is proof-based consensus, which requires the nodes joining the verifying network to show that they are more qualified than the others to do the appending work. The second group is voting-based consensus, which requires nodes in the network to exchange their results of verifying a new block or transaction, before making the final decision. For proof-based algorithms, we present PoW, PoS, and DPoS. For voting-based algorithms, we present PBFT, as an example.

For each algorithm, we present the basic idea of how to reach consensus with that algorithm and analyze corresponding energy cost, especially compared to PoW. Furthermore, we provide some real-world blockchain examples using such algorithms that make the most of the market capitalizations.

A. Proof-of-Work

Proof-of-Work (PoW) is the consensus algorithm applied by Bitcoin and many other famous cryptocurrencies such as Ethereum, Litecoin, and Zcash. In PoW, all the nodes in the network are required to solve a "puzzle" with a brute-force approach until one of them first manages to find a hash that is less than a specific hash target number. Note that although there is only one final winner for each puzzle, all of the nodes participating in solving the puzzle have to keep performing the complex computation, which means not only the final winner but also all the other nodes will consume a huge amount of energy. The difficulty of finding such a hash increases as the hash target number becomes smaller, and because of the extremely time-consuming process and rare chance to find a value, it is a proof of "work" as the miner has to spend a colossal amount of time and energy to "mine" it. Therefore, the mining process is the essential reason for the energy consumption issue.

Moreover, with the difficulty increasing, more and more complex puzzles need to be solved and the electricity consumption that comes from relentless, complex computing is bound to increase. We'll give detailed data analysis of the energy consumption of Bitcoin and Ethereum, both of which are based on PoW and have the largest market capitalization currently, in the later section.

B. Proof-of-Stake

Proof-of-Stake (PoS) is a type of consensus mechanism by which a cryptocurrency blockchain network achieves distributed consensus. In PoS-based cryptocurrencies, the creator of the next block is chosen via various combinations of random selection and wealth or age (i.e., the stake) [2].

The main differences between PoS and PoW can be listed as follows: For PoW, to add each block to the chain, miners compete to solve a difficult puzzle using their computers' processing power. For PoS, however, there is no competition on computing power as the block creator is chosen by an algorithm based on the user's stake. In terms of attack, to add a malicious block in PoW, the attacker has to own more than 51% computation power of the network. While in PoS, the attacker has to own 51% of all the cryptocurrency on

the network. Another major difference is the reward. In PoW, people get a reward for mining a block while in PoS people do not need to solve puzzles to mine blocks, so there is no reward for making a block. However, in both systems, they take the transaction fee [3].

Particularly, in terms of the energy consumption difference, in PoS, the miners do not need to solve puzzles to mine new blocks, the energy consumption and electronic waste are low compared to PoW. There has been news that Ethereum plans to cut its energy consumption by 99 percent by replacing PoW with PoS [4].

There have been many PoS based currencies since PoS was proposed. The first PoS based currency was PeerCoin [5] which kept Proof-of-Work as part of the minting process to facilitate initial minting. With the development of PoS protocol, we have NovaCoin which uses a hybrid PoS / PoW system [6]. Nowadays, some of the PoS-based cryptocurrencies that take up the most market capitalizations are Binance Coin, Polkadot, Cardano, Stellar, etc [7].

A modification of PoS is the Delegated Proof-of-Stake protocol commonly known as DPoS. Unlike the Proof-of-Stake protocol where a user puts his coins on stake for acquiring the right to validate a transaction, forge blocks, and earn associated rewards, DPoS protocol allows users to vote a witness and the witness who gets the maximum vote will get the right to validate a transaction. This protocol is also found to consume less energy as compared to Proof-of-Work and is also better than Proof-of-Stake [8]. Some of the PoS-based cryptocurrencies that take up the most market capitalizations are EOS, TRON, Tezos, etc [7].

C. Practical Byzantine Fault Tolerance

The Byzantine Fault Tolerant Algorithm (BFT) is a fault-tolerant algorithm for Byzantine problems. The BFT solution allows nodes in a network to reach a consensus when the communication is reliable but the node may be down or evil. The Practical Byzantine Fault Tolerant (PBFT) [10] is the first widely used BFT algorithm. In PBFT, if more than two-thirds of the nodes are working normally, the entire system can work well.

Specifically, one node in the system will be regarded as the master node, and the other nodes are child nodes. All nodes in the system will communicate with each other and reach a consensus on data based on the principle that the minority obeys the majority. There are four steps of establishing the consensus via PBFT. First, the client sends a request to the master node to perform an operation. Second, the master node communicates with each child node. Third, all nodes perform the algorithm and return the result to the client. Fourth, the client receives the result from nodes.

There are two main advantages of the PBFT algorithm. First, PBFT is highly efficient compared with PoW, as it does not need to wait for block confirmation and the consensus will be established instantly once the verification process of a new block is finished. Second, it is energy saving and environmentally friendly as mining is not required — no hash puzzle needs to be solved in PBFT. However, PBFT cannot be used in public blockchain since the communication cost will be extremely huge. In PBFT, the number of nodes is limited due to the needs of frequent communication between each node. What's more, the PBFT cannot prevent a malicious user from using multiple accounts to conduct consensus fraud. Consequently, User authority control should be applied to the PBFT system.

The PBFT have been widely used in blockchain applications and one of the most famous is Hyperledger Fabric. Hyperledger Fabric introduces a new blockchain architecture with elasticity, flexibility, scalability and confidentiality. Hyperledger Fabric Blockchain is a modular, extensible blockchain with access control, which supports the execution of distributed applications.

III. Energy Consumption Data Analysis

According to the statistics from Cambridge Bitcoin Electricity Consumption Index (CBECI) as shown in Fig. 1 [13], in the past five years, Bitcoin's electricity consumption has basically doubled every year. In particular, violent fluctuations occur with fluctuations in market prices.

Also, according to the Bitcoin Energy Consumption Index (BECI) Chart from Digiconomist shown in Fig. 2 [11], the peak value of the annual electricity consumption reached 77.782TWh, which is comparable to the power consumption of Chile. The generated annual carbon footprint is nearly 36.95 Mt of carbon dioxide, comparable to the carbon footprint of New Zealand. Moreover, the electricity consumption of a single transaction is 761.93 kWh, which is close to the energy consumption of 700,000 VISA payments and is equivalent to the 20-day average electricity consumption of American households, and the e-waste generated by each transaction is 101.10 grams.

As for the energy consumption of Ethereum, we can observe from the Ethereum Energy Consumption Index [12] shown in Fig. 3 that, the annual total electrical energy consumption is 11.89 TWh, which is comparable to the power consumption of Uruguay, and the footprint per single transaction is 29.44 kWh, equivalent to the power consumption of an average U.S. household over 0.99 days.

IV. Deliverables

Our deliverables will be a comprehensive, detailed paper including analysis of and comparison between different consensus algorithms, specific data and clear diagrams showing the energy consumption with different metrics, and our proposed solution to build an environmentally friendly blockchain.

V. Concrete Plans

We believe that our deliverables will be feasible. The concrete plan is shown in Fig. 4.

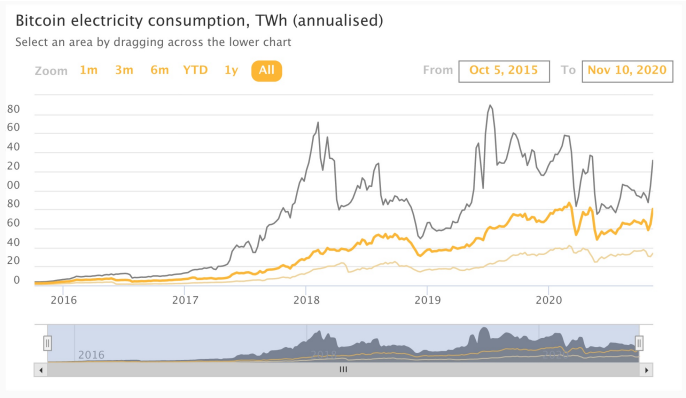

Fig. 1. Cambridge Bitcoin Electricity Consumption Index (CBECI)

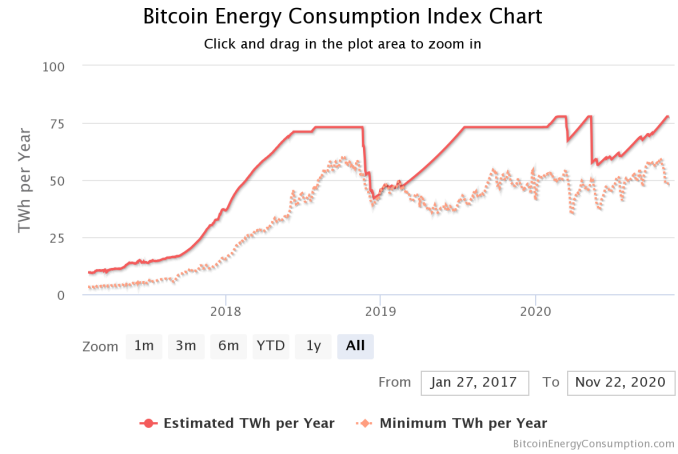

Fig. 2. Bitcoin Energy Consumption Index (BECI)

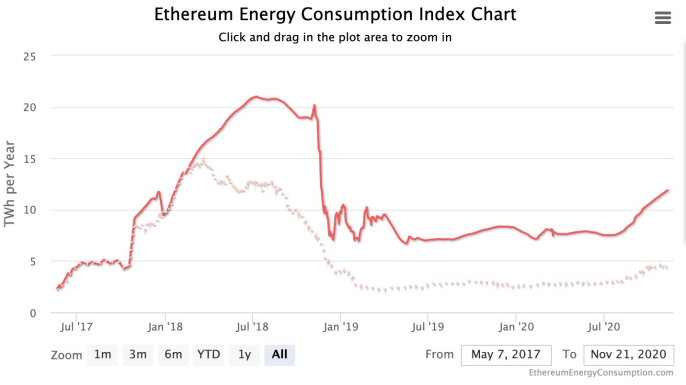

Fig. 3. Ethereum Energy Consumption Index (EECI)

Dates	Plan
10/31	Collect and read consensus algorithm papers
11/5	Finish analyzing and comparing different consensus algorithms
11/8	Grab energy consumption data with various metrics (total electricity consumption, transaction efficiency, etc)
11/9	Give a comprehensive analysis of the data
11/11	Midterm Report
11/20	Finish analyzing the source code of different consensus algorithms
11/25	Generate data visualization of energy consumption (code required)
11/29	Draw conclusion and possible solutions to build environmentally friendly blockchain
12/7	Give project presentation
12/9	Finish Final Report

Fig. 4. Concrete Project Plan

VI. Work Divided Among Members

The work is almost evenly distributed. Take the midterm report for example, we had several discussions in early October and made the agreement that each of us was responsible for collecting different consensus algorithms, such as PoS, PoW, DPoW, DPoS, PBFT. Also, each of us analyzed a part of the consensus algorithms in detail, and exchanged ideas with each other. After that, together we searched and grabbed energy consumption data of Bitcoin and Ethereum, and finished the data analysis together. Finally, each of us completed the corresponding part of the midterm report, and then proofread the other sections. Following the midterm, we'll also actively cooperate with each other on the code implementation of the data visualization as well as the building of the final solution and the final report writing.

References

[1] Nguyen G T , Kim K . A survey about consensus algorithms used in Blockchain[J]. Journal of Information Processing Systems, 2018, 14(1):101-128.

[2] Proof-of-Stake. Wikipedia; Available online: https://en.wikipedia.org/wiki/Proof- of-stake

[3] Ameer Rosic, Proof of Work vs Proof of Stake: Basic Mining Guide. Available online: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

[4] Peter Fairley. Ethereum Plans to Cut Its Absurd Energy Consumption by 99 Percent. Available online: https://spectrum.ieee.org/computing/networks/ethereum-plans-to-cut-its-absurd-energy-consumption-by-99-percent

[5] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. peercoin.net, 2013

[6] Vasin P. Blackcoin's proof-of-stake protocol v2[J]. URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf, 2014, 71.

[7] PoS Coins. Available online: https://cryptoslate.com/cryptos/proof-of-stake/

[8] SShaan Ray. What is Delegated Proof-of-Stake, 15 April 2018 . Available Online: https://hackernoon.com/what-is-delegated-proof-of-stake-897a2f0558f9
[9] B. Choi, J. Sohn, D. Han and J. Moon, "Scalable Network-Coded PBFT Consensus Algorithm," 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 2019, pp. 857-861, doi: 10.1109/ISIT.2019.8849573.
[10] M. Castro and B. Liskov. Practical Byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999.
[11] Bitcoin Energy Consumption Index. Digiconomist. 2020. Available online: https://digiconomist.net/bitcoin-energy-consumption
[12] Ethereum Energy Consumption Index. Digiconomist. 2020. Available online: https://digiconomist.net/ethereum-energy-consumption
[13] Cambridge Bitcoin Electricity Consumption Index. 2020. Available online: https://www.cbeci.org
[14] Sedlmeir J , Buhl H U , Fridgen G , et al. The Energy Consumption of Blockchain Technology: Beyond Myth[J]. Business Information Systems Engineering, 2020(2).