

TPS Analysis, Performance Indicator of Public Blockchain Scalability

Hyug-Jun Ko¹ and Seong-Soo Han^{2,*}

Abstract

In recent years, Bitcoin and Ethereum have witnessed a surge in trading activity, driven by venture capital investment and funding through initial coin offerings (ICOs) and initial exchange offerings (IEOs). This heightened interest has led to kickstarting a vibrant ecosystem for blockchain development. The total number of cryptocurrencies listed on CoinMarketCap.com has reached 2,274 highlights how dynamic and wide blockchain development landscape has grown. In blockchain development, new blockchain projects are being created by forking blockchains inspired by major cryptocurrencies such as Bitcoin and Ethereum. These projects aim to address the perceived shortcomings and improve existing technologies. Altcoins, representing these alternative cryptocurrencies, are an ongoing industry effort to improve performance and security with enhancement proposals such as Bitcoin Improvement Proposals (BIP), Ethereum Improvement Proposals (EIP), and EOSIO Enhancement Proposals (EEP). With competitive attempts to improve blockchain performance and security, an ongoing performance race between various blockchains has taken shape, each claiming its own performance advantages. In this paper, we describe the transactions contained in the blocks of each representative blockchain, and find the factors that affect the transactions per second (TPS) through transaction processing and block generation processes, and suggest their relationship with scalability.

Keywords

Bitcoin, Blockchain, EOS.IO, Ethereum, TPS

1. Introduction

In blockchain, transactions refer to actions that cause a state change as a result of processing transactions in a state, and changes in status are completed through the creation of blocks. The number of transactions that have been processed based on a unit interval of 1 second is referred to as transactions per second (TPS). To be exact, when blocks containing transactions are created, TPS are calculated and the number of transactions per block is divided by the block creation time interval.

Bitcoin, the inaugural blockchain, reached the maximum number of confirmed transactions per day of 490,644 transactions as of December 14, 2017 [1], and underwent a soft fork called SegWit on August 1, 2017 to handle the growing number of transactions [2], and the maximum daily transaction tally as of 2023 was 703,692 transactions on October 15, 2023.

Similarly, Ethereum achieved a daily peak of 1,349,890 TPS on Thursday, January 4, 2018, with the

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Manuscript received December 12, 2023; first revision December 21, 2023; accepted December 21, 2023.

* Corresponding Author: Seong-Soo Han (sshani@kangwon.ac.kr)

¹ School of Visual Information Processing, Korea University, Seoul, Republic of Korea (doltwo@korea.ac.kr)

² Division of Liberal Studies, Kangwon National University, Samcheok, Republic of Korea (sshani@kangwon.ac.kr)

GasLimit per block parameter limiting the number of transactions that can be contained in a block to prevent distributed denial-of-service (DDoS) attacks, whereas the increase in transactions has continued to grow from an initial 6 million gasses to the current 8 million level (per Etherscan), pushing the daily maximum transactions close to the daily maximum limit of 1,296,000 to 1,782,882 transactions (per Etherscan on May 8, 2021) [3]. This increase in transactions inevitably has led to a gradual increase in the size of the accumulated blocks, thus warranting storage space and increasing network latency depending on the block size. In the case of Bitcoin, for blocks with a block size of at least 20 kB, a transmission delay of 0.08 seconds occurs when the block size increases by 1 kB, so 1 MB is equivalent to a transmission delay of 80 seconds [4]. In the case of Ethereum, the uncle block will increase due to the execution of smart contract and network transfer delay [5].

As such, scaling is necessary for Bitcoin and Ethereum because the number of transactions per day is gradually increasing and approaching the maximum number of transactions per block. However, there is a problem that improving TPS performance by simply adjusting TPS parameters, such as increasing block size or adjusting block generation time to expand the number of transactions, will cause network delays [6]. Therefore, to solve this problem, this paper aims to derive an effective way to scale the performance of blockchains by analyzing blockchain transactions into transaction generation and processing, and block generation process.

2. Related Works

The blocks stored in the blockchain consist of a block header and a list of transactions processed. Because the sole purpose of blockchain is to store transactions in a safe and reliable way, transactions cannot be changed or deleted once they are created.

2.1 Bitcoin-Created Blocks

Bitcoin transmits value based on a ledger connected with a special structure called UTXO (unspent transaction output). The generic payment transaction selected from the transaction pool goes through the UTXO validation process. Transactions verified to be valid, the mining success compensation (12.5 BTC as of 2019) and the fees listed in the payment transaction are summed to generate a coin-based transaction. Using the block header generated by the coin-based transit, one or multiple nodes that have successfully found proof-of-work (PoW) among the nodes participating in mining, generate blocks at the same block height and record them in the blockchain.

PoW is done by adjusting the degree of difficulty so that it can be mined every 10 minutes on average for 2016 blocks. Change only when the block height is multiples of 2,016. If not, use the difficulty level of the previous block. The difficulty to change is handled using Formula (1):

$$New\ target = Old\ target * Total\ elapsed\ time / (14 \times 24 \times 60 \times 60) \quad (1)$$

The mining difficulty is adjusted approximately every 2016 blocks to maintain an average block time of 10 minutes, and the adjustment is based on the time it has taken to mine the previous 2016 blocks (total elapsed time) compared to the expected time (14 days, or $14 \times 24 \times 60 \times 60$ seconds). If the total elapsed

time is less than 14 days, it means that the block has been mined faster than expected and the difficulty is increased to make it harder to mine, and if the total elapsed time is greater than 14 days and the block has been mined slower than expected, the difficulty is decreased to make it easier to mine. In essence, this mechanism keeps the block generation rate close to the target of one block every 10 minutes. Fig. 1 shows bitcoin new block generation flowchart.

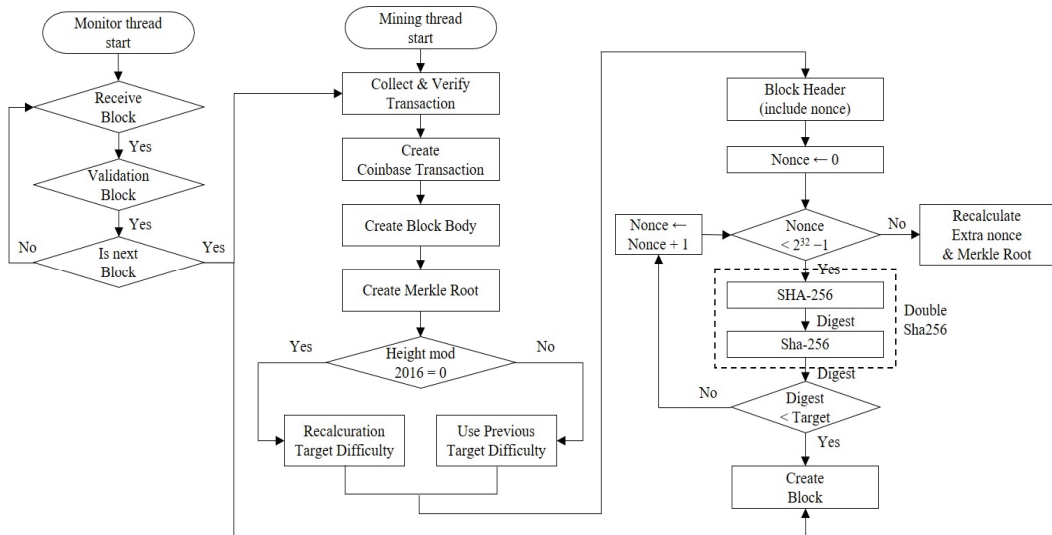


Fig. 1. Bitcoin new block generation flowchart.

2.2 Ethereum Transaction

Ethereum is based on a state machine and has a structure that performs transactions to change states and create blocks to store a state. Generated by the externally owned address (EOA) according to the entity that generates the transaction is called a transaction and classified as a message, that is an internal transaction generated by contract address (CA). A signed transaction generated by EOA is classified as a call for immediate results without the need for gas consumption, as well as transactions that generate and execute a trade-off and are sent further to another EOA. Fig. 2 shows the four types of transactions in Ethereum.

The message can call contract up to 1024 depth or perform it through call/transfer/send, which is a command that sends an immediate further message to EOA. Gas costs are deducted from the first EOA transaction call. Ethereum has been mined using “PoW” until September 15, 2022, when it reached a block height that stopped mining. Before the transition to proof-of-stake (PoS), Ethereum’s “PoW” relied on the characteristics of the state machine. Firstly, one or several nodes that configure the block header and find the nonce value through the Ethash PoW algorithm [7] run the Ethereum virtual machine (EVM) at the same block height to execute the transaction to be processed and generate a “receipt” representing the execution result. At this time, a normal transaction changes the state according to success/fail in the “receipt,” changes this state, and creates a block with a reward through the process of block finalization to store the final state. Fig. 3 shows the process by which Ethereum performs a transaction.

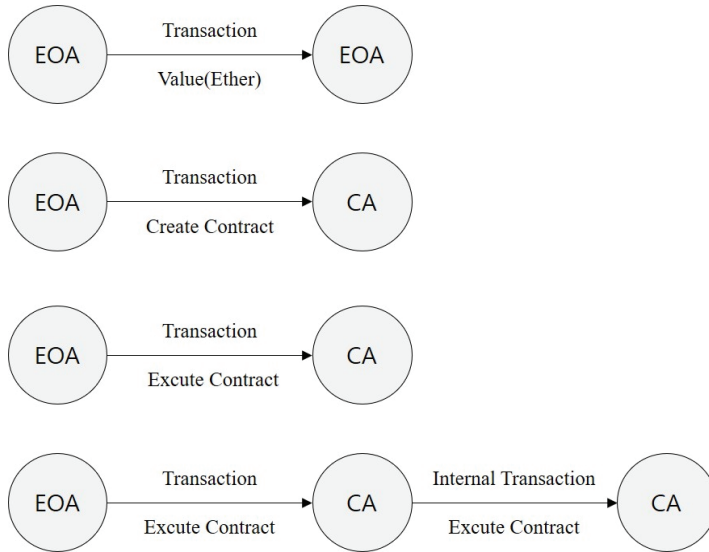


Fig. 2. Four types of transactions in Ethereum.

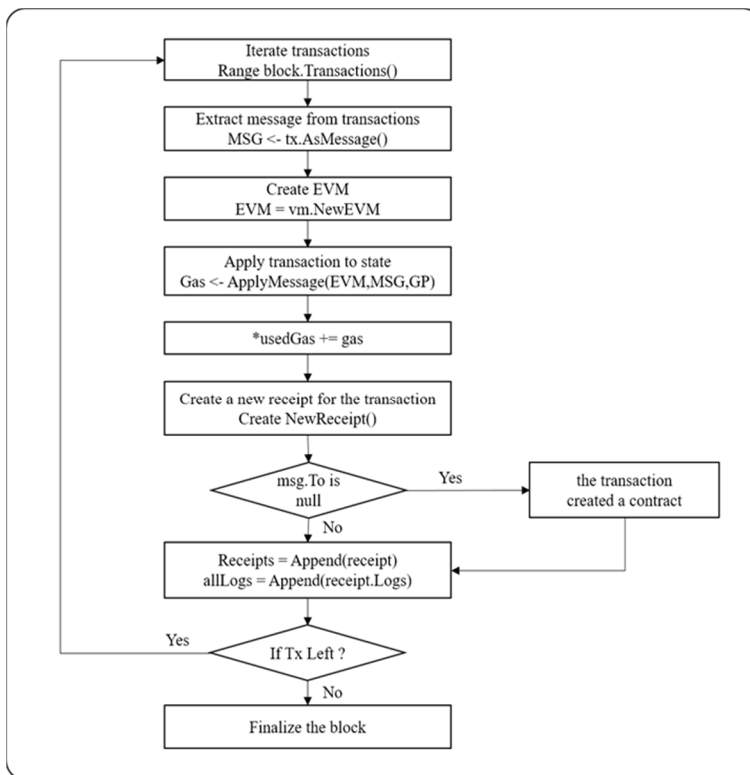


Fig. 3. Process whereby Ethereum performs transactions.

To maintain consistency in block creation time intervals, an algorithm is built into control block difficulty. If the block generation interval is less than 10 seconds, the level of difficulty increases, with the level of difficulty being maintained between 10 and 19 seconds, while the level of difficulty decreases

if it is greater than 20 seconds. According to the difficulty time bomb in every 100,000 block, it increases exponentially. The calculation formula is denoted by Formula (2) [8]:

$$\text{block_diff} = \text{parent_diff} + \text{parent_diff}/2048 * \max((1 - (\text{block_timestamp} - \text{parent_timestamp}))/10, -99) + \text{int}(2 ** (\text{block.number}/100000) - 2)) \quad (2)$$

3. TPS Analysis

Given that the TPS of blockchain indicates the transaction per second, it can be calculated by the size of the block containing the transactions and the block creation time interval, as denoted in Formula (3):

$$\text{TPS} = \frac{\text{Number of transactions in block}}{\text{Block creation time interval}} \quad (3)$$

This uses a consensus algorithm to manage the time interval of block creation, and applies the system characteristics that blockchain includes transactions in the block.

3.1 Bitcoin TPS

Bitcoin Segregated Witness (SegWit) was the first upgrade to progress on August 1, 2017, and was limited to 1 MB on August 23, 2017, when SegWit was completely activated. Currently, the concept of block size has been replaced by block weight with the use of SegWit. The block capacity is now allowed up to 4 MB, which is a 4M weight, and disk usage is approximately 2.3 MB if all transactions in one block are SegWit transactions.

Fig. 4 indicates the sample transaction's real size on disk, and over the network is 218 bytes, which is the size in bytes of the whole transaction expressed above in hexadecimal. The weight is always greater than the real size, and in this case, it is 542 weight units [9].

The algorithm proposed in this paper achieves a Bitcoin theoretical maximum speedup of about 12.3 TPS when calculated using the Bitcoin transaction denoted in Fig. 4 and calculated by Formula (4). This is a very satisfactory performance compared to the existing algorithm's Bitcoin TPS of about 3–7 TPS. In June 2019, Blockchain.com averaged 2,328 transactions per block, with an average TPS of 3.88 TPS.

When calculating the maximum TPS for Bitcoin with the transaction denoted in Fig. 4, approximately 12.3 TPS is the maximum theoretical speed. It also comprises an average of 2,328 transactions per block during June 2019 in Blockchain.com with an average TPS of 3.88 TPS.

$$\text{bitcoin TPS} = (\text{4000000 weight}/\text{512 weight})/(\text{10 minutes} * \text{60 seconds}) \quad (4)$$

```
0100000000010115e180dc28a2327e687facc33f10f2a20da717e5548406f7ae8b4c8
11072f85603000000171600141d7cd6c75c2e86f4cbf98eae221b30bd9a0b928ffff
fff019caef505000000001976a9141d7cd6c75c2e86f4cbf98eae221b30bd9a0b92
888ac02483045022100f764287d3e99b1474da9bec7f7ed236d6c81e793b20c4b5aa1
f3051b9a7daa63022016a198031d5554dbb855b8534776a4be6958bd8d530dc001
c32b828f6f0ab0121038262a6c6cec93c2d3ecd6c6072efea86d02f8e3328bbd0242
b20af3425990ac00000000
```

Fig. 4. Bitcoin sample transaction.

3.2 Ethereum TPS

Ethereum uses the method of processing transactions when inserting blocks. As a result, it is recommended to limit 4,712,388 gas per block as of May 31, 2017 when “Geth” is executed so as not to slow down the block generation speed [10].

This can involve 224 transactions per block if only the basic gas (21,000 gas) is used per transaction. In addition, according to <https://ethstats.net>, based on the actual block generation speed of 14.6 seconds (as of July 23, 2019), Ethereum can be up to about 15 TPS. The Ethereum gas limit can also change continuously at a rate of 1/1024 per block according to Formula (5):

$$Block_{gaslimit} = \frac{Parent_{gaslimit} * 1023 + Parent_{gasused} * 1.5}{1024} \tag{5}$$

Since December 13, 2017, the average gas limit based on Etherscan is about 8 million, which involves about 381 transactions per block and the maximum TPS per block is about 25.4 TPS. Upward decisions on the gas limit are based on the decision of the miner, but Ethereum's consensus algorithm, PoW, requires competition to create the blocks first for compensation. Given that an uncle block only gets a small reward, it is advantageous for the miners to have a small number of transactions in the block to shorten the transaction execution time.

3.3 EOS TPS

In order to know the TPS of EOS, it is necessary to understand how blocks are created according to the consensus algorithm, as denoted in Fig. 5.

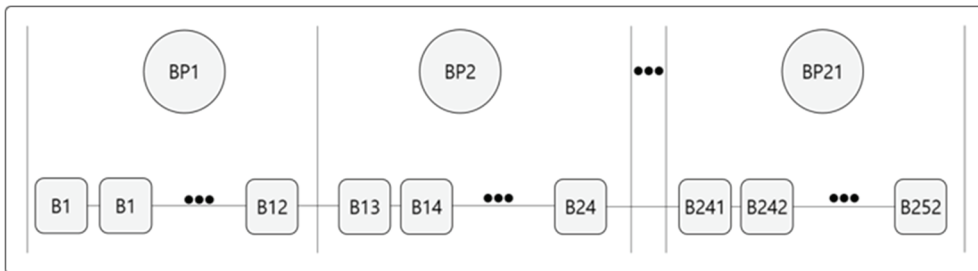


Fig. 5. EOS block produce consensus.

In EOS, the order in which blocks are created is predetermined before each round. Twelve blocks will be created in half-second intervals for the 21 top-elected block producers (BPs), and the generated blocks are passed directly to the designated nodes. This configuration also allows asynchronous processing, taking into account the next block to be created. In other words, when storing blocks like Ethereum, one BP monopolizes 12 block creation times in 6 seconds instead of processing transactions, and so a method of storing them in blocks can be used. This makes it possible to enter the maximum transaction in a specific block. As a result, block height #11,302,923 and #11,302,924 containing 1,974 and 1,998 transactions respectively, were created on August 16, 2018, 04:42:06 AM, achieving 3,972 TPS. The maximum TPS is 3,996 since the block generation interval is 0.5 seconds. Fig. 6 specifies the partition-based device discovery proposed.

4. Conclusion

In the blockchain, TPS is not an appropriate measurement basis for determining the superiority of the blockchain's performance because of showing too large of a difference depending on the consensus algorithm and the method of block creation (Bitcoin 12.3 TPS, Ethereum 25.4 TPS, EOS 3,996 TPS).

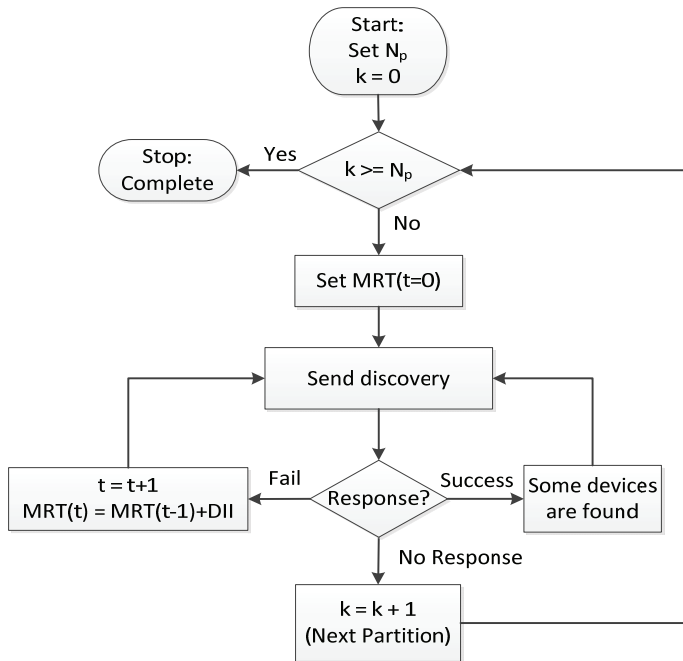


Fig. 6. Proposed partition-based device discovery.

Through this paper, we have confirmed that the three blockchains are being scaled to their respective characteristics. Bitcoin has been scaled in an approach called SegWit without adjusting the block size for scaling, Ethereum is also being scaled through GasLimit adjustment, and the transition to PoS was completed on September 15, 2022 through Casper. In the case of EOS, using the characteristics of the consensus algorithm, it was implemented by executing transactions first and generating blocks at BP's exclusive block generation time, and obtained 500–1,000 TPS, which is superior to existing blockchains. However, to achieve a higher TPS, we reduced the block generation interval from 3 seconds to 1 or 0.5 seconds, and were able to achieve up to 6 times faster TPS using a simpler formula than before.

We have shown that TPS can scale hundreds of times depending on the on-chain consensus algorithm. In conclusion, this paper reveals that TPS, the speed of a blockchain, is a valid measure of speed when compared within the same consensus algorithm. In our future work, we will study blockchain virtual machines that affect their performance within the same consensus algorithm.

Acknowledgement

This study was supported by 2020 Research Grant from Kangwon National University.

References

- [1] Blockchain.com, “Blockchain charts: confirmed transactions per day,” 2023 [Online]. Available: <https://www.blockchain.com/ko/charts>.
- [2] H. J. Ko, S. S. Han, Y. B. Jeon, and C. S. Jeong, “Bitcoin SegWit and Softfork,” in *Proceedings of the Korea Information Processing Society Conference*, Jeju, South Korea, 2019, pp. 106-109. <https://doi.org/10.3745/PKIPS.y2019m10a.106>
- [3] Etherscan, “Ethereum daily transactions chart,” 2023 [Online]. Available: <https://etherscan.io/chart/tx>.
- [4] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, “Emerging trends in blockchain technology and applications: a review and outlook,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6719-6742, 2022. <https://doi.org/10.1016/j.jksuci.2022.03.007>
- [5] K. Shah, N. Patel, J. Thakkar, and C. Patel, “Exploring applications of blockchain technology for Industry 4.0,” *MaterialsToday: Proceedings*, vol. 62, pp. 7238-7242, 2022. <https://doi.org/10.1016/j.matpr.2022.03.681>
- [6] D. P. Bauer, “Erc-721 nonfungible tokens,” in *Getting Started with Ethereum*. Berkeley, CA: Apress, 2022, pp. 55-74. https://doi.org/10.1007/978-1-4842-8045-4_5
- [7] H. J. Ko, S. S. Han, and C. S. Jeong, “Non-face-to-face P2P (peer-to-peer) real-time token payment blockchain system,” *Applied Sciences*, vol. 13, no. 13, article no. 7364, 2023. <https://doi.org/10.3390/app13137364>
- [8] M. Raikwar and D. Gligoroski, “DoS attacks on blockchain ecosystem,” in *Euro-Par 2021: Parallel Processing Workshops*. Cham, Switzerland: Springer, 2021, pp. 230-242. https://doi.org/10.1007/978-3-031-06156-1_19
- [9] S. Zhang and J. H. Lee, “Analysis of the main consensus protocols of blockchain,” *ICT Express*, vol. 6, no. 2, pp. 93-97, 2020. <https://doi.org/10.1016/j.ict.2019.08.001>
- [10] N. Lehto, K. Halunen, O. M. Latvala, A. Karinsalo, and J. Salonen, “CryptoVault: a secure hardware wallet for decentralized key management,” in *Proceedings of 2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*, Barcelona, Spain, 2021, pp. 1-4. <https://doi.org/10.1109/COINS51742.2021.9524133>



Hyug-Jun Ko <https://orcid.org/0009-0001-2901-6802>

He received dual M.S. degrees at the School of Electronic Electric Computer Engineering from Korea University in 2016 and 2018, respectively. Since September 2018, he is a Ph.D. student in the Department of Visual Information Processing at Korea University, having his current research interests in blockchain and artificial intelligence.



Seong-Soo Han <https://orcid.org/0000-0002-4915-6247>

He received an M.S. degree from Soonchunhyang University, Korea in 2005, and a Ph.D. degree from Korea University, Korea in 2019. He was a professor with Soonchunhyang University from 2018 to 2019, and is currently a professor with the Division of Liberal Studies, Kangwon National University. His research interests include computer education, artificial intelligence, blockchain, and distributed parallel processing.